CCTV Policy Statement

* 1. KL Aerial Fitness Studio uses Close Circuit Television (“CCTV”) within some of the

premises which includes the main studio area and the office/waiting area. The purpose of this policy

is to set out the position of KL Aerial Fitness Studio as to the management, operation and

use of the CCTV within the premises.

1.2 This policy applies to all members of our staff, visitors to the studio and all other persons whose images may be captured by the CCTV system.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation (“GDPR”)

1.3.2 Data Protection Act 2018 (together the Data Protection

Legislation)

1.3.3 CCTV Code of Practice produced by the Information

Commissioner

1.3.4 Human Rights Act 1998

1.4 This policy sets out the position of KL Aerial Fitness Studio in relation to its use of CCTV.

2 Purpose of CCTV

2.1 KL Aerial Fitness Studio use CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for students, staff and

visitors

2.1.2 To prevent the loss of or damage to the studio/buildings

and/or assets

2.1.3 To assist in the prevention of crime and assist law enforcement

agencies in apprehending offenders

2.1.4 To assist in the process of insurance claims for or against the business in relation to accidents or incidents on the premises resulting in injury to students or staff.

3 Description of system

3.1 Cameras have sound recording capabilities and there is a range of movable and fixed cameras.

3.2 Cameras are connected to internet via a Wifi connection with recording to a hard drive unit. Cameras can be accessed remotely via mobile view by the studio staff via a secure login.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which

the CCTV is operated. Cameras will be sited in prominent positions where

they are clearly visible to staff, students and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas

that are not intended to be the subject of surveillance.

4.3 Signs will be erected to inform individuals that they are in an area within

which CCTV is in operation.

4.4 Cameras will not be sited in areas where individuals have a heightened

expectation of privacy, such as changing rooms or toilets.

4.5 Cameras will be located in all public areas, where this is the case, employees

And students will be made aware. Access to the footage is restricted and will

only be used to fulfil the purposes in section 2.

5 Privacy Impact Assessment

5.1 Prior to the installation or repositioning of any CCTV camera, or system, a

privacy impact assessment will be conducted by the studio to ensure

that the proposed installation is compliant with legislation and ICO guidance.

5.2 The studio will adopt a privacy by design approach when installing new

cameras and systems, taking into account the purpose of each camera so as

to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system in the studio will be managed by a

Senior member of the Team.

6.2 Any allegations against staff will be referred immediately to the studio owner and only they will determine who needs to view the footage.

6.3 On a day to day basis the CCTV system will be operated by an individual with

appropriate technical ability.

6.4 The viewing of live CCTV images will be restricted (with the exception of live

CCTV positioned in external public areas) to the studio owner. In doing so they will ensure that the purposes in

2.1 are satisfied.

6.5 Recorded images which are stored by the CCTV system will be restricted as in

6.4. Relevant images may be shared with governing body panels, insurance representatives, legal representatives in relation to accidents, incidents or complaints.

6.6 No other individual will have the right to view or access any CCTV images

unless in accordance with the terms of this policy as to disclosure of images.

6.7 The CCTV system is checked daily to ensure that it is operating effectively

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as

necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored for a maximum of 60 days unless there is a specific

purpose for which they are retained for a longer period.

7.3 The studio will ensure that appropriate security measures are in place to

prevent the unlawful or inadvertent disclosure of any recorded images. The

measures in place include:

7.3.1 CCTV recording systems being located in restricted access areas;

7.3.2 The CCTV system being encrypted/password protected;

7.3.3 Restriction of the ability to make copies to specified members of

staff

7.4 A log of any access to the CCTV images, including time and dates of access,

and a record of the individual accessing the images, will be maintained by the

studio.

8 Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes

of the Data Protection Legislation, and has a right to request access to those

images.

8.2 Any individual who requests access to images of themselves will be

considered to have made a subject access request pursuant to the Data

Protection Legislation.

8.3 When such a request is made the appropriate individual with access to the

CCTV footage (ref 6.4) will review the CCTV footage, in respect of relevant

time periods where appropriate, in accordance with the request.

8.4 If the footage contains only the individual making the request then the

individual may be permitted to view the footage. This must be strictly limited

to that footage which contains only images of the individual making the

request. The individual accessing the footage must take appropriate

measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals then the studio

must consider whether:

8.5.1 The request requires the disclosure of the images of individuals

other than the requester, for example whether the images can be

distorted so as not to identify other individuals;

8.5.2 The other individuals in the footage have consented to the

disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the

circumstances to disclose those images to the individual making

the request.

8.6 A record must be kept, and held securely, of all disclosures which sets out:

8.6.1 When the request was made;

8.6.2 The process followed by to the individual with access to the CCTV

footage in determining whether the images contained third

parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and

when; and

8.6.5 Whether a copy of the images was provided, and if so to whom,

when and in what format.

Note that, when a subject access request is made then, unless an exemption applies (such as

in relation to third party data that it would be unreasonable to disclose) then the requester is

entitled to a copy in a permanent form. There is reference here only to “access” as opposed to

a “permanent copy” as the academy/Trust may consider it preferable in certain circumstances

to seek to allow access to images by viewing in the first instance without providing copies of

images. If an individual agrees to viewing the images only then a permanent copy does not

need to be provided. However, if a permanent copy is requested then this should be provided

unless to do so is not possible or would involve disproportionate effort.

9 Disclosure of Images to Third Parties

9.1 The studio will only disclose recorded CCTV images to third parties

where it is permitted to do so in accordance with the Data Protection

Legislation.

9.2 CCTV images will only be disclosed to law enforcement agencies in line with

the purposes for which the CCTV system is in place.

9.3 If a request is received from a law enforcement agency for disclosure of CCTV

images then the individual with access to the CCTV footage must follow the

same process as above in relation to subject access requests. Detail should

be obtained from the law enforcement agency as to exactly what they want

the CCTV images for, and any particular individuals of concern. This will then

enable proper consideration to be given to what should be disclosed, and the

potential disclosure of any third party images.

9.4 The information above must be recorded in relation to any disclosure.

9.5 If an order is granted by a Court for disclosure of CCTV images then this should

be complied with. However very careful consideration must be given to

exactly what the Court order requires. If there are any concerns as to

disclosure then the Data Protection Officer should be contacted in the first

instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed every two years or earlier should the need arise.

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

11.2 Any member of staff who breaches this policy may be subject to disciplinary

action.

12 Safeguarding in relation to children and vulnerable individuals

12.1 All individuals, parents and guardians will be able to view this policy prior to booking their child/looked after person into a session.

12.2 All footage recorded within the studio will be secured and inaccessible to persons other than staff within the studio.

12.3 All network connections to the CCTV system are secured appropriately using password protection and security software to prevent any other persons accessing them.

12.4 In the event of allegations or child protection enquiries/court proceedings, CCTV footage may be disclosed to police or legal persons as required by law.