CCTV

Why we use surveillance equipment,
how we protect the information it collects and
how we respond to data access requests.

ASCENSION EAGLES CHEERLEADERS
and
TALENT CENTRAL CHEER & DANCE

Last updated:

20 May 2024

Lead trustee for this policy:

Peter Sharp

TABLE OF CONTENTS

1. Who does this policy apply to? 1
2. Definition of terms used in this policy 2
    Athletes or Participants *2*
    CCTV *2*
    Controllers *2*
    Data *2*
    Data subjects *2*
    Data users *3*
    Personal data *3*
    Processing *3*
    Processors *3*
    Surveillance systems *3*
1. What this policy covers 3
2. Why this policy is important 4
3. The aims of this policy 4
4. Scope of this policy 4
5. Why we use CCTV 4
6. How we use CCTV 5
7. Retention and erasure of data gathered by CCTV 5
8. Requests for disclosure of data 5
9. Data processing 6
10. Subject Access Requests (SAR) 6
11. Requests to prevent processing 7
12. Deletion of your data 7
13. External sources of advice 7
    The Information Commissioner's Office (ICO) *7*
14. Contact information 8
15. Policy updates and next review date 8
16. The category of this policy 8
20. Change log 8

1. Who does this policy apply to?

This Policy is for and applies to:

- Ascension Eagles Cheerleaders
- Talent Central Cheer & Dance.

In this document the above will jointly be referred to as “The Group”, “We” or “Us”.

The Policy applies to any individual attending the Talent Central Cheer & Dance, including but not limited to:

- employees of The Group
- volunteers working with The Group (including trustees).

(Note that the above are collectively referred to as “employees” or “staff” in this policy)

- employees of contractors working for The Group
- professional advisers to The Group
- Parents or participants at The Group.

Wherever this document uses the expression “parent” or “parents” this includes the responsible adult/s who is/are the principal caregiver/s for a child.

2. Definition of terms used in this policy

For the purposes of this policy:

Athletes or Participants	Individuals who participate in The Group’s activities
CCTV	Means fixed and domed cameras designed to capture and record images of individuals and property.
Controllers	Are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. We are the controller of all personal data used in our business for our own commercial purposes.
Data	This means information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, “data” generally means video images. It may also include static pictures, such as printed screenshots.
Data subjects	This means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

Data users	This means our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.
Personal data	This means data relating to a living individual who can be identified from that data (or other data in our possession). This includes any video images of identifiable individuals.
Processing	This refers to any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.
Processors	These are any person or organisation which is not a data user (or other employee of a controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).
Surveillance systems	This means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future (such as automatic number plate recognition - also called ANPR - body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals).

1. What this policy covers

This policy covers the operation, and processing and storage of recordings captured by The Group's CCTV system at Talent Central Cheer & Dance, St. Mark's Industrial Estate, Unit 2J, North Woolwich Rd, London, E16 2BS.

Note: this policy does not cover the external security cameras for the St Mark's estate, which are operated by the landlord and are therefore covered by their policies for monitoring and data protection.

2. Why this policy is important

Images captured by The Group's surveillance equipment, such as CCTV, may contain images of individuals, which under data protection legislation is considered personal data. This policy is therefore intended to ensure that any images of individuals recorded by The Group's CCTV cameras and the data they collect are processed in accordance with data protection legislation.

3. The aims of this policy

The purpose of this policy is to:

- outline why and how we will use CCTV, and how we will process data recorded by CCTV cameras;
- ensure that the legal rights of Data Subjects, relating to their personal data, are recognised and respected;
- to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence; and
- explain how to make a subject access request in respect of personal data created by CCTV.

4. Scope of this policy

This policy is intended to cover any individual who is captured by surveillance monitoring equipment, such as CCTV, in operation inside the Talent Central premises (Unit 2J, St Marks Industrial Estate, North Woolwich Road, London E16 2BS).

5. Why we use CCTV

We currently use CCTV within Talent Central's general areas, which includes the front door and entrance area, the gym floor and the upstairs office area.

We believe that such use is necessary for legitimate business purposes, including:

A. to assist in day-to-day management, including ensuring the health and safety of athletes, staff and others;

B. to identify unauthorised actions or unsafe working practices that might result in disciplinary proceedings being instituted against employees and to assist in providing relevant evidence;

C. to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

D. for the personal safety of staff, visitors and other members of the public and to act as a deterrent against crime;

E. to support law enforcement bodies in the prevention, detection and prosecution of crime;

F. to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

G. Potentially to be used to review athletes' routines to identify improvement areas

H. to assist in the defence of any civil litigation, including employment tribunal proceedings;

This list is not exhaustive and other purposes may be (or become) relevant.

6. How we use CCTV

Where CCTV cameras are placed inside Talent Central, we will ensure that signs are displayed at the entrance of the surveillance zone to alert staff, athletes, parents and other visitors that they are entering an area covered by CCTV and that their image may be recorded.

We will ensure that live feeds from cameras and recorded images are only reviewed by approved members of staff whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

To protect and prevent unauthorised access to the CCTV, the system is password protected. Footage is only accessible via on premises access.

Access to footage is purely for the reasons outlined in point 7. Should a situation arise, footage may be exported, but will be transferred to an encrypted media to prevent unauthorised access to that footage.

7. Retention and erasure of data gathered by CCTV

As the recording system records digital images, any CCTV images that are held on the hard drive of a personal computer or server are deleted and overwritten on a 30-day recycling basis and, in any event, are not held for more than a three-month period, unless required. Once the hard drive has reached the end of its use, it will be erased prior to disposal.

At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or disks will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

8. Requests for disclosure of data

Access to, and disclosure of images recorded on CCTV is restricted. This ensures that the rights of individuals are retained. Images can only be disclosed in accordance with the purpose for which they were originally collected.

Disclosure of images to other third parties will only be made in accordance with the purpose for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service
- Relevant legal representatives
- Line manager's or Welfare Officers involved with The Group's disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

The Group's Director or Chair of Trustees are the only people who are permitted to authorise disclosure of images to external third parties such as law enforcement agencies.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

No images from CCTV will be posted online or disclosed to the media.

9. Data processing

The Group will process the personal data collected (which is limited to CCTV footage) in connection with the operation of
the CCTV policy in accordance with its data protection policy and any internal privacy notices in force at the relevant time.

Inappropriate access or disclosure of this data will constitute a data breach and should be reported immediately to the Director (email: director@ascensioneagles.com) in accordance with The Group's data protection policy. Reported data breaches will be investigated and may lead to sanctions under The Group's disciplinary procedure.

10. Subject Access Requests (SAR)

Under the UK's data protection laws, including the General Data Protection Regulation (GDPR), individuals have the right on request to receive a copy of the personal data that The Group holds about them, including CCTV images if they are recognisable from the image.

If you wish to access any CCTV images relating to you or your child, you must make a written request to The Group's Data Protection Officer via the email address in the contact information section of this policy.

The Group may charge a reasonable fee if you make a request which is manifestly unfounded, excessive, or is repetitive.

So that the images can be easily found and your identity can be confirmed as the Data Subject (ie you or your child is the person in the images) your request must include:

- the date and approximate time when the images were recorded and
- the location of the particular CCTV camera.

The Group will acknowledge the request within one month of receiving a request and will provide a timeframe when the request will be completed, if it is possible to do so.

The Group will always check the identity of the Data Subject making the request before processing it.

The Director or Chair of the Board of Trustees will always determine whether disclosure of your images will reveal third party information, as you have no right to access CCTV images relating to other people. In this case, the images of third parties may need to be obscured, if it would otherwise involve an unfair intrusion into their privacy.

If the Group is unable to comply with your request because access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders, you will be advised accordingly.

11. Requests to prevent processing

We recognise that, in rare circumstances, individuals may have a legal right to request erasure of personal data concerning them or to restrict the processing of their personal data. Any individual who considers that these rights apply to them in relation to our use of CCTV should contact our Data Protection Officer in the first instance.

12. Deletion of your data

Data collected from the point at which the individual makes the report will be held securely and only accessed by, and disclosed to, those individuals who require access for the purposes of dealing with the disclosure (e.g. to conduct an investigation, to keep you informed about progress/the outcome etc).

13. External sources of advice

The Information Commissioner's Office (ICO)	The Information Commissioner's Office is the UK's independent authority, set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

14. Contact information

The Director:	Angela Green
Email:	director@ascensioneagles.com
Data Protection Officer	Paula Brown
Contact no: Email:	07866 612610 paula@ascensioneagles.com

15. Policy updates and next review date

This policy will be reviewed every year in May, or whenever there is a major change in the organisation, in relevant legislation or relevant legislation or any changes in the cheerleading industry.

This policy was updated on:	20 May 2024
Updated by:	Angela Green, The Director
Reviewed by:	Paula Brown, Data Protection Officer
Other reviewers:	Sue Winston, Chair of Trustees
	Peter Sharp, Trustee
Approved by the Board:	28 May 2024
Next review due:	May 2025
To be reviewed by:	Angela Green, The Director
Review to be approved by:	The Board of Trustees

16. The category of this policy

This policy is categorised as:

Category	Description
1.	This document is publicly available and is published on the AEC website

20. Change log

The following changes have been made since this policy was last approved by the Board.

Date	Location in this document	Details of change