The Clacton Pier Company Ltd

CCTV Surveillance Policy

The Clacton Pier Company Ltd remain committed to upholding the highest standards in both Health and Safety and Security for all employees, visitors and contractors.

In this policy, the following definitions shall apply:

Site: Clacton Pier

1 INFORMATION ABOUT US

1.1 Clacton Pier/'Us'/'We'/'CPC': The Clacton Pier Company Limited (Company No. 06675051) whose registered office address is at No 1 North Sea, Clacton-on-Sea, Essex CO15 1QX

1.2 We are active members of The British Association of Leisure Parks, Piers and Attractions (BALPPA), British Amusement Catering Trade Association (BACTA) and The International Association of Amusement Parks and Attractions (IAAPA). We also participate in the UK's Amusement Device Inspection Procedures scheme (ADIPS) to ensure that our rides are certified and safe to operate. Our CCTV system provides additional peace of mind and helps us provide a safe and secure environment for our employees and visitors alike whilst also helping to manage staff and efficiencies.

1.3 We will continue to review all of our security arrangements regularly and update and implement any measures to enhance security.

1.4 You are admitted to this Site subject to our Entry Conditions (see separate policy). If you do not comply with them, you may be removed from the Site by Clacton Pier personnel, security or police officers, without any right to a refund. This is without prejudice to any claim that we may have against you or arising out of your actions. Whilst inside the Site, you must comply with any reasonable instructions given to you by Clacton Pier personnel or any third party instructed on behalf of Clacton Pier.

2 CCTV POLICY STATEMENT

2.1 This policy seeks to ensure that the Closed Circuit Television (CCTV) system used at the Site is operated in compliance with the law relating to data protection, i.e. the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It takes into account best practice as set out in codes of practice issued by the Information Commissioner (ICO)[1] and by theHome Office.[2]

2.2 CPC seeks to ensure, as far as reasonably practicable, the safety and security of all staff, visitors and contractors that use CPC's premises; and the security of its property and premises. CPC therefore deploys CCTV to:

promote a safe environment and to monitor the safety and security of its premises

assist in the prevention, investigation and detection of crime

assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings;

assist in the investigation and breaches of its policies by staff and contractors and, where relevant and appropriate, investigating complaints;

assist in the investigation of accidents.

dealing with queries, complaints and enquiries.

2.3 This policy will be reviewed annually by the Management Team and the Data Protection Officer (DPO). The Head of Administration and Office Management (HOAM) will undertake this role with guidance from the Directors to assure compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV remains justified.

2.4 CPC has carried out a legitimate interests assessment for operating CCTV in its premises. This can be found at Appendix 1. We also have a check list which is included at Appendix 2.

3 SCOPE

3.1 This policy applies to the CCTV systems in the parts of the Site owned by CPC.

3.2 This policy does not apply to other parts of the seafront and public highway abutting the front of the property forecourt, and the main entrance area, which are maintained by Tendring District Council and Essex County Council as seafront promenades, beaches and Public Highway.

3.3 This policy applies to all CPC staff and contractors.

1 https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/coronavirus-recovery-data-protection-advice-for-organisations/surveillance/
2 https://www.gov.uk/government/consultations/surveillance-camera-code-of-practice/draft-updated-surveillance-camera-code-of-practice-accessible-version

4 ROLES AND RESPONSIBILITIES

4.1 The CPC Directors are responsible for ensuring that the CCTV system, including camera specifications for new installations, complies with the law and best practice referred to in 2.1 of this policy. They are responsible for the safety and security of the equipment and software utilised for the capture, recording and playback of live and historical CCTV images.

4.2 The CPC Directors are responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the appropriate software. The list of locations and the list of people authorised to view CCTV images is maintained by the HAOM on behalf of the CPC Directors. Plans showing the location of CCTV cameras can be found at Appendix 3 [internal version only].

4.3 Changes in the use of CPC's CCTV system can be implemented only in consultation with CPC's DPO and HAOM.

5 SYSTEM DESCRIPTION

5.1 CPC operates cameras at the entrances to the Pier and at strategic locations across the Site including Discovery Bay Soft Play Centre, Skull Point Adventure Golf, Captains Table Main concourse, Arcade, The Lanes Bowling, Adult Gaming Area, Boardwalk Bar, Sunshine Terrace, Jurassic Pier, Ride Deck, Pier Head and Berthing Arm. Cameras also operate in key offices e.g. CDM room, Security Office, Stock Room, Food and Beverage Storage. They continuously record activities in these areas.

5.2 CCTV cameras are not installed in areas in which individuals would have an expectation of privacy, such as toilets. Cameras are only located so that they capture images relevant to the purpose the system was set up for. No covert recording is undertaken. Audio is recorded.

5.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed, so that staff, visitors and contractors are made aware that they are entering an area covered by CCTV. The signs include contact details of the DPO, as well as a statement of purposes for the use of CCTV.

5.4 Staff must be familiar with the policy and the procedures to be followed in the event an access request is received from either a data subject or a third party.

6 OPERATING STANDARDS

6.1 Equipment and access

6.1.1 The images are stored on a Network Video Recorder (NVR) which is located in the secured CCTV Server Room.

6.1.2 Images are accessible using the appropriate software and with an authorised username and password from specific devices. There is also a mobile app for use on a mobile phone, but this must only be used on CPC mobile phones.

6.1.3 Only authorised personnel in secured areas have access to the CCTV images. Recorded images only can be viewed in the CCTV Server Room.

6.2 Processing of recorded images

6.2.1 CCTV images are available only to persons authorised to view them (see above) or to persons who otherwise have a right to view them, such as police officers or any other person with statutory powers of entry. If such visitors are given access toview footage, their identity and authorisation must be checked, and a log retained – See 8 below.

6.2.2 Where authorised persons access or monitor CCTV images on desktops or laptops, they must ensure that images are not visible to unauthorised persons, for example by minimising screens when not in use or when unauthorised persons are present. Screens must always be locked when unattended.

6.3 Quality of recorded images

6.3.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended to be used. The standards to be met (in line with the codes of practice referred to in 2.1) are set out below:

- recording features such as the location of the camera, date and time reference must be accurate and maintained
- consideration must be given to the physical conditions in which the cameras are located, i.e. additional lighting or infrared equipment may be needed in poorly lit areas, and
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept.

6.4 Retention and disposal

6.4.1 CCTV images are not to be retained for longer than necessary, taking into account the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a 30 day rotation in data retention.

6.4.2 If there is a legitimate reason for retaining the CCTV images (such as for use in an accident investigation, disciplinary investigation and/or legal proceedings), the footage or still frames can be isolated and saved outside the DVR to a separate encrypted zip file. Any saved images or footage will be deleted once they are no longer needed for the purpose for which they were saved.

6.4.3 All retained CCTV images will be stored securely.

7 DATA SUBJECT RIGHTS

7.1 Recorded images, if sufficiently clear, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.

7.2 Data subjects have a right to access to their personal data under the data protection legislation. They also have other rights, in certain circumstances, including the right to have their data erased, rectified, and to restrict processing and object to processing. They can ask to exercise these rights by emailing the HAOM – info@clactonpier.co.uk.

7.3 On receipt of a request – which needs to include the date and approximate time of the recording – the HAOM will liaise with the Directors and the Property Services Manager regarding compliance with the request and communicate the decision to the data subject. This should be done without undue delay and at the latest within one month of receiving the request unless an extension of the period is justified.

7.4 If a request is to view footage, and the footage only contains the individual concerned, then the individual may view the footage. The authorised person accessing the footage must ensure that the footage available for viewing is restricted to the footage containing only the individual concerned.

7.5 If the footage requested contains images of other people, the HAOM must consider:

- whether the images of the other people can be distorted so as not to identify them
- seeking consent from the third parties to their images being disclosed to the requester, or
- if these options are not possible, whether it is reasonable in the circumstances to disclose the images to the individual making the request in any case.

7.6 The HAOM will keep a record of all disclosures which sets out:

- when the request was made and by whom
- what factors were considered in deciding whether to allow access to any third party images
- whether the requester was permitted to view the footage, or if a copy of the images was provided, and in what format.

Requesters are entitled to a copy in permanent form. If a permanent copy is requested, this should be provided unless it is not possible to do so, or it would involve disproportionate effort. (For example, it may be acceptable to allow a requester to view footage which contains third party images, but not to provide a permanent copy.)

8 THIRD PARTY ACCESS

8.1 Third party requests for access will usually only be considered, in line with the data protection legislation, in the following categories:

- from a legal representative of the data subject (letter of authorisation signed by the data subject would be required);
- from law enforcement agencies including the police;
- disclosure required by law or made in connection with legal proceedings;
- HR staff responsible for disciplinary and complaints investigations and related proceedings;
- Staff employed by our contractors responsible for disciplinary and complaints investigation and related proceedings concerning their own staff.

8.2 Where images are sought by other bodies/agencies, including the police, with a statutory right to obtain information, evidence of that statutory authority will be required before CCTV images are disclosed.

8.3 The HAOM will consider disclosing recorded images to law enforcement agencies once a form certifying that the images are required for one of the following reasons has been received:

- an investigation concerning national security
- the prevention or detection of crime, or
- the apprehension or prosecution of offenders,

and that the investigation would be prejudiced by failure to disclose the information. The HAOM will also need to take into account the guidance regarding "Requests for Information from the Police", as necessary.

8.4 Where third parties are included in images as well as the person who is the focus of the request, the same considerations need to be made as in the case of subject access requests.

8.5 Every disclosure of CCTV images (including where authorised persons are given access to view footage in the Security Office) is recorded in the CCTV Operating Log Book and contains:

- the name of the police officer/other relevant person receiving the images
- brief details of the images captured by the CCTV including the date, time and location of the footage/images
- the purpose for which they will be used
- the crime reference number where relevant, and
- date and time the images are handed over to the recipient.

9 COMPLAINTS PROCEDURE

9.1 Any complaints relating to the CCTV system should be directed in writing to the HAOM promptly and in any event within seven days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month of the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office.

9.2 Complaints in relation to the release of images should be addressed to the HAOM. These will be responded to promptly and, in any event, within 30 days of receipt. They will be dealt with in accordance with the provisions of the UK GDPR and theData Protection Act 2018 (or any successor legislation).

10 OTHER

10.1 These terms and conditions and all matters arising under it shall be governed by English Law and the parties submit to the Jurisdiction of the High court of Justice in England and Wales

Version 4 : Policy Issue Date 6th April 2023
Author / Originator: William Ball – Data Protection Officer

Policy Review Date: 6th April 2024

This document is to be used for staff circulation and website publication.

Appendix 1

Legitimate Interest Assessment for operating CCTV on Pier premises

The Clacton Pier Company Ltd operates CCTV cameras at the entrances to the Pier and at strategic locations across the premises, including Discovery Bay, Adventure Golf, Captains Table Main Concourse, Arcade, The Lanes Bowling, Adult Gaming Area, Boardwalk Bar, Sunshine Terrace, Jurassic Pier, Ride Deck, Workshop, Jolly Roger, Pier Head and Berthing Arm. Cameras also operate in key offices e.g. CDM room, Security Office, Stock Room, Food and Beverage Storage.

Identify the legitimate interests

Why do we want to process the data – what are we trying to achieve?

CCTV is operated in the building primarily for security and safety reasons, to protect employees, visitors and contractors. Occasionally, CCTV images may also be used in HR disciplinary or accident investigations involving visitors, our own staff or staff of our contractors.

Who benefits from the processing? In what way?

The primary beneficiaries are our staff and visitor by enabling them to be secure. The presence of the CCTV will also help to give a perception of security and safety. Where HR are investigating a disciplinary matter where there has been a dispute between members of staff, the processing will benefit/protect the injured party in the dispute. This is also the same for accident/incident investigations involving visitors or staff.

Are there any wider public benefits to the processing?

Yes - processing helps to ensure the safety of anyone visiting the attraction, and in helping to keep the premises safe this adds to the overall feeling of security on the site for our visitors.

How important are those benefits?

They are hugely important as we are committed to delivering a safe and secure environment for our visitors to come and enjoy the attraction. We also hope that this is also adopted by our employees to uphold a positive and proactive safety culture

What would the impact be if we couldn't go ahead?

Safety and security within the site may be compromised. We may not be able to prove allegations made against staff or the general public without CCTV evidence which in turn allows us to improve the level of customer experience and high level of safety that we strive to achieve.

Would our use of the data be unethical or unlawful in any way?

No, our use of CCTV complies with the ICO's Surveillance Camera Code of Practice and the Home Office's Data Protection Advice for Organisations. .The system does use Wi-Fi and transmits encrypted images securely over the internet. The device that stores the images is located in the locked comms room.

The necessity test

Does this processing actually help to further that interest?

Yes, for the reasons given above.

Is it a reasonable way to go about it?

Yes.

Is there another less intrusive way to achieve the same result?

No, there is no alternative to achieving the same result.

The balancing test

Consider the impact of our processing and whether this overrides the interest we have identified. We might find it helpful to think about the following:

What is the nature of our relationship with the individual?

Our relationship with the individual is either as employer or organisation responsible for the safety, security and wellbeing of visitors.

Is any of the data particularly sensitive or private?

No, we are only recording images of staff, visitors and contractors to the site in public and common areas. Any recordings in the key offices or stock rooms are staff and contractors. Recordings are available on a live feed and kept for 30 days. After that period they are overwritten. This is considered the shortest reasonable time to allow for requests for the images to be made and dealt with, for example, if an accident has taken place and it is necessary to review what happened.

Would people expect us to use their data in this way?

Yes, we display notices as appropriate and systems such as these are common place in public attractions for all of the reasons outlined above.

Are we happy to explain it to them?

Yes, we include information on our use of CCTV in our privacy notices, and we have a CCTV Policy.

Are some people likely to object or find it intrusive?

We have not had any objections from our staff as all reasons and procedures have been fully explained and understood. We anticipate this to be the case with our visitors.

What is the possible impact on the individual?

The impact on the individual is only likely to be positive as we seek to provide a safe environment for them whilst they are working or visiting. However, if they have been

investigated for a company breach of policy or procedure which we deem to be severe, this may help us in identifying potential safety or security, welfare or equality issues.

How big an impact might it have on them?

Under normal circumstances, the impact is likely to be very small. It will only have a significant impact if the person filmed breaching health and safety policy or procedures (see above). If they are an intruder or someone else has acted inappropriately towards them our CCTV images may provide evidence of a disciplinary offence and disciplinary measures could be taken against the offender.

Are we processing children's data?

Yes, we are processing children's data. Please see Safeguarding Policy.

Are any of the individuals vulnerable in any other way?

It is possible some individuals may be vulnerable. Please see Safeguarding Policy.

Can we adopt any safeguards to minimise the impact?

The impact is already minimised in that CCTV is only operating with the clear objective to promote health and safety of our employees, visitors and contractors.

Can we offer an opt-out?

No.

LIA Carried out by: William Ball
16/02/2023

Appendix 2

Checklist for users of limited CCTV systems

This CCTV system and the images produced by it are controlled by Martin Taylor, Property Services Manager, who is responsible for how the system is used, along with approved managers or individuals under his direction.

We (CPC) have considered the need for using CCTV and have decided it is required on our site for the safety and security of our employees, visitors and contractors. Also, for the prevention, investigation and detection of crime. See our Legitimate Interests Assessment for Operating CCTV. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

		Checked (date)	By	Date of next review
There is a named individual who is responsible for the operation of the system.	Martin Taylor Property Services Manager	15/02/2023	DPO	February 2024
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.	See our Legitimate Interests Assessment for Operating CCTV	15/02/2023	DPO	February 2024
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.	System supplied by Berserk Security	15/02/2023	DPO	February 2024
Cameras have been sited so that they provide clear images.	Yes	15/02/2023	PSM & DPO	February 2024
There are visible signs showing that CCTV is in operation.	Yes, signage is at the front of the Pier	15/02/2023	PSM	February 2024
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.	Stored on Digital Video Recorder linked to Network. Only access by Facilities staff	15/02/2023	DPO	February 2024

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.	Images retained for 30 days – but can be extended if further investigation needed, or images can be downloaded	15/02/2023	DPO & PSM	February 2024
Except for law enforcement bodies, images will not be provided to third parties.	Under Health & Safety Law, RIDDOR images need to be available. Contractually Images need to be available to insurance companies	15/02/2023	HOAM & PSM	February 2024
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.	Yes, see Legitimate Interests Assessment	15/02/2023	DPO & HOAM	February 2024
CPC knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.	Yes, as long as request made within 30 days. Can easily isolate frames and save to encrypted zip file.	15/02/2023	HOAM & PSM	February 2024
Regular checks are carried out to ensure that the system is working properly and produces high quality images.	Checks normally carried out quarterly.	15/02/2023	PSM & HOAM	February 2024

Please keep this checklist in a safe place until the date of the next review.

DPO: Mr William Ball

PSM: Mr Martin Taylor

HOAM: Mrs Sharon Charters