CCTV Policy

Authorisation and Amendment Record

Version No.	Reason for Re-Issue	Date of Re-issue:	Prepared By:	Authorised By:	Signed:
0	Not applicable. First Draft	N/A	VR	VS / SJ	
1	Implementation	22/06/21	SJ	S Joyce	
1	Update	21/09/21	SJ	S Joyce	

Policy Statement

1.1. This policy seeks to ensure that the Closed-Circuit Television (CCTV) system used at the Cirque Skills Pathway CIC 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 the Home Office (2)

1 https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf (2017)
2 www.gov.uk/government/publications/surveillance-camera-code-of-practice (2013) CCTV Policy

1.2. Cirque seeks to ensure, as far as reasonably practicable, the safety and security of all staff and all others that use Cirque's offices; and the security of its property and premises. Cirque therefore deploys CCTV to:

- promote a safe office 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, students and contractors and, where relevant and appropriate, investigating complaints;
- assist in the investigation of accidents.

The Directors of Cirque reserve the right to utilise the CCTV footage in the public areas of the centre to assist in the investigation of any issues raised by staff, students or their parents or guardians.

1.3. This policy will be reviewed annually by Directors to assure compliance with clauses 1.1 and 1.2 and to determine whether the use of the CCTV remains justified.

2. Scope

2.1. This policy applies to the CCTV systems in the parts of 2nd Floor Silver House, Silver Street, Doncaster, DN1 1HL

2.2. This policy does not apply to other parts of the building, including the exterior and the main entrance area, which are maintained by the landlord.

2.3. This policy applies to all Cirque staff, students and contractors.

3. Roles and Responsibilities

3.1. The 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 1.1 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.

3.2. The Directors are responsible for the evaluation of locations where live and historical CCTV images are available for viewing via the appropriate software. There are cameras in each room and three in the hallway. There are no cameras in the spray tanning room and the toilets.

3.3. Changes in the use of Cirque's CCTV system can be implemented only in consultation with the Board of Directors.

4. System Description

4.1. The Cirque operates cameras at the entrance of the centre and in all communal areas. They record activities in these areas based on motion detection and for five minutes after the last motion detected. (Other cameras operate in other locations in the building which are operated and controlled by the building's landlord.)

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

4.3. CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed at the entrance and around the building, so that staff, visitors, and contractors are made aware that they are entering an area covered by CCTV. The sign inside the main entrance door includes contact details of the director responsible for the CCTV system, as well as a statement of purposes for the use of CCTV.

5. Operating standards Equipment and Access

5.1. The images are stored on a Digital Video Recorder (DVR) which is in a securely locked room.

5.2. Images are accessible using the appropriate software and with an authorised username and password from Directors' laptops. There is also a mobile app for use on a mobile phone which can only be accessed from the Director's mobile phones.

5.3. Only Directors have access to the CCTV images unless for a legitimate Police or data access request as detailed herein

Processing of Recorded Data

5.4. 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 to view footage, their identity and authorisation must be checked, and a log retained – see 7 below.

5.5. 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.

Quality of recorded images

5.6. 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 1.1) 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.

Retention and Disposal

5.7. CCTV images are not to be retained for no longer than the recording capacity of the DVR recorder. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce a rotation in data retention.

5.8. 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.

5.9. All retained CCTV images will be stored securely.

6. Data Subjects Rights

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

6.2. 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 Directors on info@cirque.org.uk.

6.3. On receipt of a request – which needs to include the date and approximate time of the recording – the above-named Director will liaise with the rest of the Board of Directors 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.

6.4. 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.

6.5. If the footage requested contains images of other people, the Director 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.

6.6. The Directors 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.)

7. Third Party Access

7.1. 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, and
- Staff employed by our contractors responsible for disciplinary and complaints investigation and related proceedings concerning their own staff.

7.2. 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.

7.3. The Directors 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
- the apprehension or prosecution of offenders, and that the investigation would be prejudiced by failure to disclose the information.

7.4. 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.

7.5. Every disclosure of CCTV images (including where authorised persons are given access to view footage in the Director's 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.

8. Complaints Procedure

8.1. Any complaints relating to the CCTV system should be directed in writing to the Directors. A complaint will be responded to in line with the company complaints policy which is available by asking the Directors or can be downloaded from www.cirque.org.uk.

8.2. Complaints in relation to the release of images should be addressed to the Directors. These will be responded to promptly and, in any event in line with the company complaints policy. They will be dealt with in accordance with the provisions of the UK GDPR and the Data Protection Act 2018 (or any successor legislation).

8.3 Cirque Skills Pathway CIC is registered with the ICO for its use of CCTV recording in its premises.