CCTV POLICY

Responsible for Implementation: Director of Planning and Operations
Latest Review Date: January 2023
Next Review Date: January 2024
Authorised By: Director of Planning and Technical Operations
Version 1.2

Contents

About Us

Access to Music Limited ('The College') has subsidiary companies, trading names and trading partnerships through which it operates. The trading names and partnerships might have their own names or brands, but the legal entity for the purpose of this policy is Access to Music Limited. Trading subsidiaries, trading names and trading partnerships include Access Creative College ('ACC'), National College for Creative Industries ('NCCI'), and Access Sport.

Introduction

Access To Music Ltd ('The College) is the "data controller" for your personal data under the applicable legislation and it is primarily responsible for processing and ensuring proper protection of your data.
The College owns and operates a closed-circuit television ("CCTV") scheme (the "CCTV Scheme").

The purpose of this policy is to:

- Outline the College's CCTV Scheme
- Comply with the requirements of the UK GDPR and Data Protection Act 2018
- Set out the responsibilities of all employees (including temporary and contract staff) who are responsible for for implementing, managing, operating or using the CCTV Scheme

This policy is to be read in conjunction with the Appendices below.

The CCTV Scheme

The CCTV Scheme comprises a number of cameras, installed at strategic locations. Cameras will either record in colour or black and white and are fixed. We do not record audio via CCTV at any of our sites.
The College's CCTV Scheme may result in the processing of images from which specific individuals may be identified and which fall within the definition of 'personal data' as defined in the UK GDPR and Data Protection Act 2018.
The purposes of the CCTV Scheme are to:

- Help ensure a safer environment and reduce fear of crime
- Help with our health and safety obligations and requirements
- Facilitate the prevention and detection of crime, including the identification, apprehension and prosecution of offenders
- Assist with the investigation of potential breaches of The College's regulations are/or actions which may result in disciplinary proceedings against students or staff

The purpose for processing this information is for security and safety reasons. The lawful basis we rely on to process this personal data is legitimate interests.
The Scheme will not normally be used for routine workforce monitoring or for covert monitoring. Covert monitoring will only take place under exceptional circumstances, e.g. where there is an expectation of financial crime being committed, and will be undertaken subject to professional legal advice.
The CCTV Scheme cannot prevent, cover or detect every incident which occurs within The College and/or the areas covered by the Scheme.

Responsibilities

The Director of Planning and Technical Operations is responsible for the overall management and operation of the CCTV Scheme, with support from the Director of Estates and Resources, the IT and Infrastructure Manager, the Data Protection Team, the Data Protection Officer, and the Director of People Services.
In each local centre the Resources Manager will be responsible for the operations of CCTV. If the Resources Manager experiences any technical difficulties with the CCTV system they should contact the Director of Planning and Technical Operations without delay.
All employees (including temporary and contract staff) who are responsible for operating or using the CCTV Scheme must do so only as authorised and must be appropriately trained.
Failure to comply with this policy may result in disciplinary action and/or criminal liability.

Impact Assessment

The College carries out an assessment prior to installation of CCTV cameras, and reviews the Scheme periodically, to ensure adequate and appropriate use and compliance with the purposes for the CCTV Scheme as set out in section 2 of this policy and relevant legislation, as set out in section 1 of this policy.
Where practicable, cameras are restricted to the College premises, which may include outdoor areas and does include corridors and entrances to rooms. CCTV is very rarely used in standard classrooms. If a classroom is in an open plan space, then part of the classroom may be covered. Cameras are also positioned in the recording studios and IT rooms, as these are high value locations and likely to be the focus of out-of-hours crime. Members of staff have access to details of where CCTV cameras are situated, with the exception of any cameras placed for covert monitoring, in exceptional circumstances as detailed in section 2.
The College is not responsible for CCTV equipment, which may be installed in the common areas of shared facilities and buildings and these are not covered under this Scheme. The College may liaise with building owners / landlords where necessary to obtain legitimate access to their CCTV for the purposes set out under this Scheme.

Signage

The College notifies individuals whose images may be captured by the CCTV Scheme of the use of CCTV and its purposes, by means of this policy and by CCTV warning signs which are prominently placed in external places close to The College's entrances. Signs are legible, visible, appropriately sized, relevant to the location, confirm that The College operates the CCTV, indicate the purposes of the Scheme, and who to contact regarding the Scheme.
There are some sites where learners, staff and visitors' images are captured under external CCTV, for example where CCTV systems and notices are managed by landlords of properties we use to deliver services. See Appendix A for further information.

Equipment and Images

The CCTV Scheme's equipment is appropriate to ensure that images are adequate for the purpose for which they are obtained. For crime detection and prevention purposes, images are sufficiently clear to be able to identify individuals and to be used in evidence. CCTV cameras are checked for any damage by centre managers and IT support checks that images are captured correctly periodically.
CCTV images are not retained for longer than necessary for the purposes for which the images were recorded. The retention period is 30 days.Occasionally, images (which are downloaded within this retention period) may be retained for longer to meet the purposes for which the images were taken, e.g., for investigating a crime or disciplinary matter.
CCTV images are kept securely.The CCTV streams are encrypted with a keyphrase \ password so that anything outside of the network needs a password to view live streams or playback recordings. Connection to the cameras is encrypted. Peer to Peer communication protocol is disabled.
CCTV footage is typically saved in a proprietary format that is unreadable \ unplayable using traditional third party media players.
Hikvision Cameras are completely 'closed circuit' and not connected to the Local Area Network. Ubiquiti UniFi cameras use end to end WebRTC encryption. Secure Real Time Protocol (SRTP) encryption and other security standards are mandated for all WebRTC sessions. Video streams on Unifi Systems are also DTLS encrypted and therefore cannot be viewed without the encryption key. Datagram Transport Layer Security is a communications protocol providing security to datagram-based applications by allowing them to communicate in a way designed to prevent eavesdropping, tampering, or message forgery.

The CCTV Scheme does not include areas requiring a heightened expectation of privacy (such as changing rooms or toilet areas).

All employees and workers responsible for managing, operating or otherwise using CCTV are trained in connection with this Policy.

Access to /disclosure of images

Access to viewing recorded footage will be restricted to those staff authorised to view them and will not be made more widely available, but requests for disclosure under certain circumstances can be made in accordance with this policy (see below). All requests for access to footage will be reviewed in line with the organisation's CCTV Protocol and Procedure.
All requests for disclosure must be made in writing, including reasons / justification for the request and, where possible, relevant exemptions under the Data Protection Act / other legislation. All requests should be referred to the Data Protection Team dataprotection@accesstomusic.ac.uk who will decide (in consultation with other departments and legal advisors where appropriate / necessary) whether a disclosure can be made. More information can be found on our DSAR Policy on our Microsite.
The College retains discretion to refuse any request for information unless there is an overriding legal obligation (e.g. court order or information access rights).
A record of all requests for disclosure is retained, together with the reasons for disclosure or refusing the request.
There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to The College where these would reasonably need access to the data (e.g. investigators).
CCTV images/recordings may also be used within The College's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

Data Subject Access Requests

Individuals whose images are recorded have a right to request access to data containing images of themselves. Requests should be made to the Data Protection Team by emailing dataprotection@accesstomusic.ac.uk The College will aim to respond within a calendar month. The person making the request must supply sufficient information to enable The College to identify them as the subject of the images, including the date / time / location, physical description and photograph. Data subjects are not entitled to receive images / personal data of any third party.
As a general rule, if the viewer can identify any person other than, or in addition to, the person requesting access,and if it is not possible to conceal the identity of others, disclosure is unlikely. Refusal to disclose footage, even if no other person is identifiable, may be appropriate where its release is:

- Likely to cause substantial and unwarranted damage to an individual.
- To prevent automated decisions from being taken in relation to an individual.
- Likely to prejudice the legal rights of individuals or jeopardise an ongoing investigation.

Contacts and Complaints

Enquiries about the operation of CCTV within The College should initially be directed to the Centre Manager at The College's premises, who will refer any requests to the Data Protection Team.
For all CCTV enquiries, The College can also be contacted on 0800 281842
Complaints about the operation of CCTV within The College should be directed to the Data Protection Team dataprotection@accesstomusic.ac.uk
Any complaint with regard to any aspect of the CCTV Scheme, will be investigated and dealt with in accordance with the complaints, concerns and compliments policy and procedures of The College ccc.admin@accesstomusic.ac.uk
If necessary, individuals can obtain more information by contacting the Information Commissioner's Office via https://ico.org.uk/make-a-complaint/

Appendix A

SCHEDULE OF CCTV CAMERA SITES

Signage will be on display at The College's premises which use CCTV, stating:

1. That the area is covered by CCTV surveillance and pictures are recorded
2. The purpose of using CCTV
3. The name of the organisation.
4. The contact telephone number or address for enquiries

Where any CCTV is not owned and operated by The College (for example, where premises are owned and operated by another organisation) the building owners will manage the CCTV system and appropriate signage. By way of example, York Access Creative College has 3 external cameras operated by the Jam Factory. A list of these premises is available on request.

Certain premises which own and operate CCTV are also used by other organisations. For any requests or enquiries relating to CCTV footage at our sites, please contact dataprotection@accesstomusic.ac.uk.

The locations of The College's owned and operated CCTV sites are:

- Birmingham - 68 Heath Mill Ln, Deritend, Birmingham, B9 4AR
- Bristol -All Saints St, Bristol BS1 2LZ
- Lincoln - 32 Clasketgate, Lincoln, LN2 1JS
- London - 50 Hoxton St, London , N1 6LP
- Manchester - St James Bldg, 65 Oxford St Manchester M1 6FQ
- Manchester - 24 Hulme Street, Manchester M1 5BW
- Manchester - 50 Fountain Street, Manchester M2 2AS
- Norwich - 114 Magdalen St, NR3 1JD
- Liverpool - Brookfield drive, 17-19 Wareing Rd, Aintree, L9 7AU

Appendix B

SCHEDULE OF AUTHORISED CCTV STAFF

The following job roles have CCTV authorisation:

- Centre Managers / Heads of Centre (for premises where The College owns and operates CCTV equipment)
- Members of the Executive Leadership team (if required)
- Head of Estates
- Head of IT
- Head of Sport
- Data Protection Officer
- Systems Administrator
- Centre based Resource Managers (in each centre)

Appendix C

SCHEDULE OF CCTV DATA RETENTION AND DISPOSAL

CCTV footage is recorded and saved onto the secure hard drive of each centre, for a retention period of 30 days. Once the hard drive is full, the oldest footage is overwritten. Access is restricted to the IT and Infrastructure Manager, the Network Engineer and the Centre based Resource Manager.
In the event that an office or site closes permanently, the standard retention period will be observed with footage from the last day of operation being retained for 30 days after closure.