Closed Circuit Television Policy

Policy name: Closed Circuit Television Policy

Approved by Trinity Academic Council 13th May 2020

1. Context

1.1 Closed Circuit Television Systems (CCTVS) are installed in the Royal Irish Academy of Music's (hereinafter referred to as RIAM or the Academy) premises located at 36-38 Westland Row, Dublin 2, D02 WY89.

1.2 New CCTV systems will be introduced in consultation with staff. Where systems are already in operation, their operation will be reviewed regularly in consultation with staff.

2. Purpose

2.1 The purpose of this policy is to regulate the use of Closed Circuit Television and its associated technology in the monitoring of both the internal and external environs of the premises.

2.2 CCTV systems are installed (both internally and externally) in the premises for the purpose of enhancing security of the staff, the building and its associated equipment, as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises 24 hours per day.

2.3 CCTV surveillance at RIAM's premises is intended for the purposes of:

(i) protecting buildings and assets, both during and after hours;

(ii) promoting the health and safety of staff, students and visitors;

(iii) preventing bullying;

(iv) reducing the incidence of crime and anti-social behaviour (including theft and vandalism);

(v) supporting the Gardaí in a bid to deter and detect crime;

(vi) assisting in identifying, apprehending and prosecuting offenders;

(vii) ensuring that RIAM's rules are respected so that the organisation can be properly managed.

3. Scope

3.1 This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in rented premises, the RIAM will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

3.2 All employees have a responsibility to adhere to this policy and failure to do so may result in disciplinary action, up to and including dismissal.

4. Principles

4.1 RIAM as the corporate body has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its staff, students and visitors to its premises.

4.2 RIAM owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of staff and students, by integrating the best practices governing the public and private surveillance of its premises.

5. Policy

5.1 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

5.2 Information obtained through the CCTV system may only be released when authorised by the RIAM Secretary. Any requests for CCTV recordings/images from An Garda Síochána will be fully recorded and legal advice may be sought as deemed appropriate (see 'Access' at 6.7.2(i) below). If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, they may require a warrant and accordingly any such request from them should be made in writing, and RIAM may seek legal advice as deemed appropriate.

5.3 Video monitoring of public areas for security purposes within RIAM's premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

5.4 RIAM reserves the right to use information obtained in accordance with the terms of this policy in any disciplinary proceedings against an employee or a student of RIAM.

5.5 All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by RIAM. Recognisable images captured by CCTV systems are 'personal data. They are therefore subject to the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

6. Procedures

6.1 The Data Protection Act 2018 requires that data is "adequate, relevant and not excessive" for the purpose for which it is collected. This means that RIAM needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV to control the perimeter of the buildings for security purposes has been deemed to be justified by the Board of Governors. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

6.2 CCTV systems will not be used to monitor normal teacher/student classroom activity. In other areas of the buildings where CCTV has been installed, e.g. hallways, stairwells, locker areas, the RIAM Secretary has demonstrated that there is a proven risk to security and/or health and safety, and that the installation of CCTV is therefore proportionate in addressing such issues.

6.3 *Location of Cameras*

6.3.1 The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. RIAM has endeavoured to select locations for the installation of CCTCV cameras which are least intrusive to protect the privacy of individuals.

6.3.2 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

6.3.3 CCTV video monitoring and recording of public areas in RIAM may include the following:

(i) *Protection of buildings and property*: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services.

(ii) *Monitoring of Access Control Systems*: monitor and record restricted access areas at entrances to buildings and other areas.

(iii) *Verification of Security Alarms*: Intrusion alarms, exit door controls, external alarms.

(iv) *Video Patrol of Public Areas*: Parking areas, main entrance/exit gates, traffic control.

(v) *Criminal Investigations (carried out by An Garda Síochána*): robbery, burglary and theft surveillance.

6.4 *Covert Surveillance*

6.4.1 RIAM will not engage in covert surveillance.

6.4.2 Where An Garda Síochána requests to carry out covert surveillance on RIAM premises, such covert surveillance may require the consent of a judge. Accordingly, any such request received from An Garda Síochána should be in writing, and RIAM may seek legal advice as deemed appropriate.

6.5 *Notification – Signage*

6.5.1 The RIAM Secretary will provide a copy of this CCTV Policy on request to staff, students, parents and visitors to the Academy. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be indicated to the Board of Governors.

6.5.2 Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to RIAM property.

6.5.3 Signage shall include the name and contact details of the Data Controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

6.6 *Storage and Retention*

6.6.1 The Data Protection Act 2018 states that data shall not be kept for longer than is necessary for the purposes for which it was obtained. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft, and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

6.6.2 Accordingly, the images captured by the CCTV system will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

6.6.3 The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the RIAM Secretary, who may delegate the

administration of the CCTV System to another staff member. In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above (such individuals may include the Gardaí, the Director, the Administrative Officer, the relevant Head of Faculty, other members of the teaching staff, representatives of the Department of Education and Skills, representatives of the HSE and/or the parent of a recorded student). Any employee who uses the CCTV system or CCTV images in an unauthorised manner may be subject to disciplinary action up to and including dismissal. Unauthorised use is any processing incompatible with the data's original purpose including, but not limited to:

(i) disclosure of images containing personal data to an unauthorised third party, including other employees;

(ii) unauthorised processing of personal data in the form of copying the images on to a disk, website or print format;

(iii) circulation of images containing personal data by email or posting of images containing personal data on the internet.

6.6.4 When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

6.6.5 Tapes/DVDs will be stored in a secure environment with a log of access to tapes kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

6.7 *Access*

6.7.1 Tapes/DVDs storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.

6.7.2 Access to the CCTV system and stored images will be restricted to authorised personnel only. In relevant circumstances, CCTV footage may be accessed:

(i) by An Garda Síochána, in accordance with the procedures set out at 5.2 above; or

(ii) following a request by An Garda Síochána when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on RIAM's property; or

(iii) by the HSE and/or any other statutory body charged with child safeguarding; or

(iv) to assist the Director/RIAM Secretary in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed; or

(v) by data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to RIAM; or

(vi) by individuals (or their legal representatives) subject to a court order; or

(vii) by RIAM's insurance company where the insurance company requires access in order to pursue a claim for damage done to the insured property.

6.7.3 *Access requests*: On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted, and provided also that an exemption/prohibition does not apply to the release. Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the RIAM Secretary. RIAM must respond within 28 days**.** Individuals should specify whether they would be satisfied with merely viewing the images rather than requiring a copy

6.7.4 Access requests may be made to the RIAM Secretary at RIAM, 36-38 Westland Row, Dublin 2, D02 WY89 or via email to kevinkelleher@riam.ie .

6.7.5 A person should provide all the necessary information to assist RIAM in locating the CCTV recorded data, such as the date, time and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be released by RIAM. Individuals requesting access to images must supply RIAM with the following:

(i) adequate information for the images to be located;

(ii) sufficient information to enable RIAM to verify that the applicant has a legitimate right to request access;

(iii) proof of identification through photographic identification, for example passport or driving license.

6.7.6 In giving a person a copy of their data, RIAM may provide a still/series of still pictures, a tape or a disk with relevant images. However, other images of other individuals will be obscured before the data is released.

6.7.7 In the event that a request for access is denied, RIAM will document the following:

(i) the identity of the individual making the request;

(ii) the date of the request;

(iii) the reason for refusing to supply the images requested.

The document will then be signed and dated and will be provided to the individual making the data access request.

7. Responsibility

7.1 The RIAM Secretary is responsible for overseeing this policy and as part of this brief shall:

(i) ensure that the use of CCTV systems is implemented in accordance with the policy set down by RIAM;

(ii) oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within RIAM;

(iii) ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy;

(iv) ensure that the CCTV monitoring at RIAM is consistent with the highest standards and protections;

(v) review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy;

(vi) maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system;

(vii) ensure that monitoring recorded tapes are not duplicated for release;

(viii) ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally;

(ix) provide a list of the CCTV cameras and the associated monitoring equipment and the capabilities of such equipment, located in RIAM;

(x) approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events. [*Note: Temporary cameras do not include mobile video equipment or hidden surveillance cameras used for authorised criminal investigations by An Garda Síochána.]*

(xi) give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment;

(xii) ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within RIAM and be mindful that no such infringement is likely to take place;

(xiii) co-operate with the Health and Safety Officer in reporting on the CCTV system in operation in RIAM;

(xiv) advise the Department of Education and Skills that adequate signage at appropriate and prominent locations is displayed as detailed above;

(xv) ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of 'Reasonable Expectation of Privacy';

(xvi) ensure that monitoring tapes are stored in a secure place with access by authorised personnel only;

(xvii) ensure that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 28 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other *bona fide* use as approved by the Chair of the Board;

(xviii) ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy;

(xix) ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics;

(xx) ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas;

(xxi) ensure that where An Garda Síochána request to set up mobile video equipment for criminal investigations, legal advice has been obtained and such activities have the approval of the Chair of the Board.

7.2 The RIAM CCTV system is controlled by a security company contracted by RIAM as follows:

(i) RIAM has a written contract with the security company in place which details the areas to be monitored, how long data is to be stored, what the security company may do with the data, what security standards should be in place and what verification procedures apply. The security company has undertaken to give the RIAM all reasonable assistance to deal with any subject access request made under GDPR and the Data Protection Act 2018 within the statutory time-frame (generally 40 days).

(ii) Security companies that place and operate cameras on behalf of clients are considered to be Data Processors. Staff of the security company have been made aware of their obligations relating to the security of RIAM data. As data processors, they operate under the instruction of the Data Controller i.e. RIAM.

(iii) GDPR and the Data Protection Act 2018 place a number of obligations on data processors. These include having appropriate security measures in place to prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network and against all unlawful forms of processing. This obligation can be met by having appropriate access controls to image storage or having robust encryption where remote access to live recording is permitted.

7.3 *Contact Details*

Data Controller: Kevin Kelleher at email: kevinkelleher@riam.ie
Data Protection Officer: Theresa Doyle at email: theresadoyle@riam.ie

8. Legislation and Regulation

8.1 Safety, Health and Welfare at Work Act 2005.

8.2 Equality & Diversity Policy.

8.3 Dignity at Work Policy.

8.4 Codes of Practice.

8.5 General Data Protection Regulation (GDPR).

8.6 Data Protection Act 2018.

9. Related Documents

9.1 Data Protection Policy.

9.2 Records Management and Retention Policy.

10. Review

10.1 This policy will be reviewed on a three year cycle, or as required to take into account changes in the law and the experience of the policy in practice.

11. Document Control

Approved by Trinity Academic Council 13th May 2020.
Next review: Academic Year 2020/2021.

Glossary of Terms

CCTV – Closed-circuit television is the use of video cameras to transmit a signal to a specific place on a limited set of monitors. The images may then be recorded on video tape or DVD or other digital recording mechanism.

Data Protection Act 2018 – The Data Protection Act 2018 confers rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

General Data Protection Regulation (GDPR) - This legislation emphasises transparency, security and accountability by data controllers and processors, while at the same time standardising and strengthening the right of European citizens to data privacy. The GDPR also increases the range of possible sanctions for infringements of these rules.

Data Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under the Data Protection Act 2018.

Data Processing - performing any operation or set of operations on data, including:

- obtaining, recording or keeping the data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The GDPR and Data Protection Act place responsibilities on such entities in relation to their processing of the data.