RCSI CCTV Policy

RCSI DEVELOPING HEALTHCARE LEADERS WHO MAKE A DIFFERENCE WORLDWIDE

Contents

1. Introduction

Closed Circuit Television Systems (CCTV) are installed in Royal College of Surgeons in Ireland (RCSI) for the purposes outlined in section 3 of this policy.

All CCTV systems, under the control of RCSI, will operate in compliance with the Data Protection Acts 1988 to 2018 and will only be used for the purposes specified in this policy.

2. Purpose & Scope of this Policy

The purpose of this policy is to inform staff of the correct usage of and access to the CCTV system, and to ensure that authorised third party contractors are aware of their duties and responsibilities when using RCSI's CCTV system.

This policy relates to the location and positioning of CCTV cameras, the usage of the CCTV system and the monitoring, recording, retention and subsequent usage of such recorded material, in compliance with Data Protection legislation.

3. CCTV Purposes

CCTV at RCSI is used for the purposes of:

- protecting college property and assets
- promoting the health and safety of staff, students and the general public;
- investigating insurance claims;
- preventing crime and anti-social behaviour (including theft and vandalism);
- supporting the Gardai in their role to prevent and/or investigate criminal activity; and
- ensuring that the College rules are respected and upheld

4. Proportionality & Legitimate Usage of CCTV Monitoring

A privacy impact assessment has been carried out on the existing CCTV system by the Records & Information Compliance Manager in conjunction with Estates and Support Services to ensure that the monitoring and usage of the CCTV system is proportionate to the CCTV principles outlined above, whilst safeguarding the privacy of those individuals identifiable.

This privacy impact assessment will be reviewed on an annual basis and new cameras or new positioning of existing cameras will be reviewed on an individual basis.

CCTV monitoring of public areas is limited to uses that do not violate the individual's reasonable expectation of privacy.

5. Notification – Policy and Signage

RCSI will provide a copy of this CCTV Policy on request to staff, students and the general public. In addition a copy of same is available on the staff and student portals.

Adequate signage is positioned and prominently displayed at all RCSI entrances. Signage shall include the name and contact details of the data controller (RCSI) as well as the specific purpose(s) for the CCTV system. The exact positioning of the signage is detailed in the privacy impact assessment.

WARNING
CCTV cameras in operation
Images are being monitored and recorded for the purpose of crime-prevention, for the safety of our staff and students and for the protection of RCSI and its property.
This scheme is controlled by RCSI Estate and Support Services Department and operated by Security Service provider.
For more information contact Estate and Support Offices 01 4022101

6. Security of CCTV system

The monitoring equipment and related digital footage is securely stored in a restricted access area. Unauthorised access to this area is not permitted at any time. The area is locked when not occupied by authorised personnel. A log of access to CCTV images and recordings is maintained, and only possible via password.

7. Storage and Retention of CCTV images

The images captured by the CCTV system will be retained for a maximum of 30 days, after which time they will be automatically overwritten. Where an issue has been identified which requires further investigation using CCTV images, and which is in line with the purposes specified in this policy, images will be specifically retained in the context of an investigation/prosecution of that issue.

The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. It is the responsibility of the Estate and Support Services department to supervise the access and maintenance of the CCTV System. Estates and Support Services delegate the administration of the CCTV System to specific managers within the department; day-to-day operation and surveillance of the CCTV system is contracted to a third party security provider.

Secure measures will be employed when using disk storage, with automatic logs of access to the images created.

8. Covert Surveillance

RCSI does not engage in covert surveillance.

Where An Garda Síochána request to carry out covert surveillance from RCSI premises, such covert surveillance will be formally requested by appropriate senior members, District / Station Superintendent from An Garda Síochána to Estate and Support Services and authorised / approved by same.

9. Access

Authorised access

Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. designated Managers within Estate and Support Services and approved RCSI contract security staff.

CCTV footage may be accessed in line with CCTV principles and in the following circumstances:

- By An Garda Síochána where RCSI are required, by law, to make a report regarding the commission of a suspected crime;
- 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 / near RCSI property,
- To assist the relevant appropriately appointed College Officer in establishing facts in cases of suspected breach of RCSI's Student Code of Conduct;
- To assist the relevant appropriately appointed staff or externals in establishing facts in cases of suspected breach of relevant RCSI's policies and procedures;
- To data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished to RCSI,
- To individuals (or their legal representatives) subject to a court order;
- To investigate insurance claims.

Requests by An Garda Síochána

Any requests for CCTV recordings/images from An Garda Síochána must be supported by a declaration, in writing, from the appropriate District / Station Superintendent confirming that CCTV is required as part of an investigation. This is retained on file by the Estates and Support Services Office for a duration of 3 years, after which time it is destroyed.

RCSI Staff request for access as part of an investigation

In certain circumstances as deemed necessary, the recordings may also be viewed by appropriately appointed College Officers in line with the CCTV principles set out in section 3.

Any requests for CCTV recordings/images from RCSI staff must be supported by a declaration, in writing (email), confirming that CCTV requests form part of an investigation – investigation pertaining to crime-prevention, safety of our staff and students, for the protection of RCSI and its property or to investigate suspected breach of RCSI's Student Code of Conduct. This request is retained on file by the Estates and Support Services Office.
When CCTV recordings are being viewed, access will be limited to authorised individuals.

Access requests under Data Protection Acts or Freedom of Information Act:

On written request, any person whose image has been recorded can make a request under the Data Protection Acts or Freedom of Information Act for recordings in which they are identifiable. 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 RCSI Records & Information Compliance Manager.

Information obtained through the CCTV system may only be released when authorised by the nominated RCSI Estate and Support Services Managers – Building and Estates Manager, Front of House Manager or Engineering Manager, in conjunction with RCSI Legal Counsel.

10. Responsibilities

Estate and Support Services will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within RCSI
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- 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
- Ensure that recorded images are not duplicated for release
- Ensure that the perimeter of view from fixed location cameras both internally and externally do not unnecessarily invade the privacy of the individual
- Maintain a list of the CCTV cameras and associated monitoring equipment located in RCSI and the capabilities of such equipment
- 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].
- 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
- Ensure that adequate signage at appropriate and prominent locations is displayed
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing
- Ensure that monitoring recording are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on DVDs/digital recordings are stored for a period not longer than 30 days and are then erased unless required in line with the CCTV principles outlined in section 3 of this policy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. in line with CCTV policy and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- 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 RCSI Legal Counsel.

11. Security Companies and Service Providers

The CCTV system in RCSI is controlled by a Private Security Authority licensed security company contracted by Estate and Support Services. The following applies:

RCSI has a written contract with the security company 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 written contract also states that the security company will give RCSI all reasonable assistance to deal with any subject access request made under applicable legislation which may be received by RCSI.

Security companies that place and operate cameras on behalf of RCSI are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). Applicable legislative requirements 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. Staff of the security company have been made aware of their obligations relating to the security of data.

12. Implementation & Review

The policy will be reviewed and evaluated from time to time. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, audit recommendations (internal and external to RCSI), legislation and feedback from students, staff and others.

Appendix 1 – Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy;

- 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.
- The Data Protection Acts 1988 to 2018 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. RCSI staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the organisation and individuals who interact with the organisation.
- 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.
- Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under the Data Protection Acts.
- 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 Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

Appendix 2

RCSI CCTV Privacy Impact Assessment

Prior to installing new CCTV, the following privacy impact assessment is carried out.

This is an important procedure as a contravention may result in action being taking against RCSI by the Office of the Data Protection Commissioner, or may expose the college to a claim for damages.

Proposed Camera location:	

1. What is the purpose for using / installing additional CCTV images? What are the issues/problems it is meant to address?

2. Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?

3. Is it justified under the circumstances?

4. Where is the purposed location?

5. Who will have access to the system and recordings/images?

6. What security measures are in place to protect the CCTV system and recordings/images?

7. Are those who will have authorised access to the system and recordings/images clear about their responsibilities?

8. Does RCSI procedure ensure that recordings/images are erased or deleted as soon as the retention period (30 days) has expired?

Camera location confirmed:	**Yes** / No
Privacy Impact Assessment created by:	
Approved by:	

Appendix 3 – Risk assessment

Risk no.	Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
		Remote, possible or probable	Minimal, significant or severe	Low, medium or high
1	Accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, CCTV recordings.	Remote	Significant	Medium
2	Lack of privacy information leading to non-compliance with first data protection principle i.e., requirement to ensure processing is fair, lawful and transparent.	Remote	Significant	Medium
3	Local installation of surveillance equipment without Estate and Support Services involvement.	Remote	Significant	Medium
4	Excessive data capture e.g., placement of multiple cameras covering one location or capture of footage 24 hours per day 7 days per week.	Possible	Minimal	Low
5	Excessive data retention i.e., retention of surveillance footage for longer than needed.	Remote	Minimal	Low
6	Excessive sharing within RCSI i.e., as a result of failure to lock-down access on a need-to-know basis.	Remote	Significant	Medium
7	Unlawful sharing with 3rd parties i.e., disclosure to third parties without appropriate GDPR safeguards in place.	Remote	Significant	Medium

8	Privacy intrusion e.g., location of cameras near accommodation block windows, private residences, in changing rooms, toilets etc.	Remote	Significant	Medium
9	Poor quality recordings unable to fulfil their intended purpose.	Possible	Minimal	Low
10	Risk that CCTV is renewed and/or installed without following policy requirements e.g., undertaking a DPIA to minimise privacy risk.	Remote	Minimal	Low
11	Risk of function creep i.e., reuse of surveillance footage for a secondary, incompatible purpose.	Remote	Significant	Medium

Appendix 4 – Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk				
Risk	**Options to reduce or eliminaterisk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, Medium or High	Yes/no
1	All footage is stored securely on University servers or a secure cloud. Access to footage is restricted to authorised personnel in line with CCTV policy and GDPR requirements.	Reduced	Low	Yes
2	Privacy notices published and communicated to data subjects widely e.g., via campus signage.	Reduced	Low	Yes
3	All works on campus are coordinated and approved solely by Estate and Support Services and their function is to identify the need for CCTV installation, thus ensuring compliance with this DPIA and a consistent approach.	Reduced	Low	Yes
4	Careful consideration during renewal/first time installation to ensure the number of cameras in situ is not excessive. RCSI CCTV Privacy Impact Assessment checklist is completed to ensure all installations are (a) fit for purpose and (b) not excessive and (c) not privacy intrusive.	Reduced	Medium	Yes

5	Agreed retention periods are set out in this CCTV policy. Deletion is automated so risk of excessive retention is low. Where records have been manually flagged for extended retention, standard operating procedures will ensure they are deleted as soon as they are no longer required.	Reduced	Low	Yes
6	Access is restricted as outlined under Access within this CCTV policy. When CCTV is being reviewed by Estate and Support Services staff measures are taken to restrict viewings to those authorised to do view same.	Reduced	Medium	Yes
7	Access will be restricted on a need-to-know basis. Records of any 3rd party disclosure will be maintained by Security team and communicated to Estate and Support Services.	Reduced	Medium	Yes
8	Camera locations are not located where privacy intrusion may occur.	Reduced	Low	Yes
9	Chosen surveillance hardware is fit for purpose i.e., can record footage at a high enough quality to support the purpose.	Reduced	Low	Yes
10	In line with CCTV policy a CCTV Privacy Impact Assessment checklist is completed to ensure all installations are (a) fit for purpose and (b) not excessive and (c) not privacy intrusive.	Reduced	Low	Yes
11	Accepted uses for surveillance footage are set out in this CCTV policy thus the risk of secondary re-use is low as all.	Reduced	Low	Yes