Athlone Institute of Technology

CCTV Policy

Revision 3.0
Revision History

Date of this revision: 24th February 2020  Date of next review: February 2021

<table>
<thead>
<tr>
<th>Version Number/Revision Number</th>
<th>Revision Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.0</td>
<td>4th October 2018</td>
<td>Initial Document Version</td>
</tr>
<tr>
<td>Revision 2.0</td>
<td>11th January 2019</td>
<td>See Consultation History</td>
</tr>
<tr>
<td>Revision 3.0</td>
<td>24th February 2020</td>
<td>See Consultation History</td>
</tr>
</tbody>
</table>

Version 2.0 11th January 2019 See Consultation History

Consultation History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Consultation Date</th>
<th>Names of Parties in Consultation</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feb – Sept 2018</td>
<td>Estates Manager, Data Protection Officer, VP Financial and Corporate Affairs, HR Manager, Commercial Manager</td>
<td>Initial Document Version</td>
</tr>
<tr>
<td>2</td>
<td>2 October 2018 – January 2019</td>
<td>Estates Manager, Data Protection Officer, VP Financial and Corporate Affairs, HR Manager</td>
<td>Number layout, Combine similar sections, Remove duplicate information</td>
</tr>
<tr>
<td>3</td>
<td>February 2020</td>
<td>Estates Manager, Assistant Buildings Officer, VP Financial And Corporate Affairs</td>
<td>Upgrade of policy to enable Contractors avail of campus systems for security purposes; inclusion of section 2.1.7 and 4.9, Document formatted</td>
</tr>
</tbody>
</table>

Approval

This document requires the following approvals:

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Management Team</td>
<td>15th January 2019</td>
</tr>
<tr>
<td>Executive Management Team</td>
<td>3rd March 2020</td>
</tr>
</tbody>
</table>

This Policy was agreed by the Executive Management Team on 3rd March 2020. It shall be reviewed periodically and, as necessary, amended by the Institute. All amendments shall be recorded on the revision history section above.

Appendices

Appendix A. Privacy Risk Assessment
Appendix B. CCTV Footage Access Request Form
Appendix C. CCTV System Access Log Sample
Appendix D. CCTV Footage – Confidentiality Agreement
Appendix E. CCTV Usage by Subsidiary Companies CSS and AIT Sportsco
Table of Contents

1. Introduction 4
2. Purpose of Policy 4
3. Scope 4
4. General Principles 4
5. Justification of Use of CCTV 5
6. Location of Cameras 6
7. Surveillance and Criminal Investigation 6
8. Notification of Signage 6
9. Data and Storage Retention 7
10. Access 7
11. Responsibilities of the Estates Manager 9
12. Security Companies and Data Protection 10
13. Implementation and Review 10
1. Introduction

1.1 Closed Circuit Television Systems (CCTV) are installed and operate in Athlone Institute of Technology.

2. Purpose of Policy

“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 under the remit of Athlone Institute of Technology”

2.1 CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating an awareness 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 during both the daylight and night hours each day. CCTV surveillance at the Institute is intended for the purposes of:
2.1.1 Protecting the Institute buildings and assets, both during and after Campus opening hours;
2.1.2 Promoting the health and safety of staff, students and visitors;
2.1.3 Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
2.1.4 Supporting the Gardaí in a bid to deter and detect crime;
2.1.5 Assisting in identifying, apprehending and prosecuting offenders; and
2.1.6 Ensuring that relevant Institute policies, procedures and guidelines are respected so that the Institute can be properly managed.
2.1.7 To provide additional security for works contractors sites on campus

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 Institute activities are carried out in off campus premises, the responsible person of that activity will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

4. General Principles

4.1 Athlone Institute of Technology has a statutory responsibility for the protection of its property, equipment and other plant as well providing a sense of security to its employees, students and invitees to its premises. Athlone Institute of Technology 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 the campus community by integrating the best practices governing the public and private surveillance of its premises.
4.2 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.
4.3 Information obtained through the CCTV system may only be released when authorised by the Estates Manager, or Vice President for Financial and Corporate Affairs, (or a Vice President in
his/her absence, following consultation with the President (or a Vice President in his/her absence) of the Institute. Any requests for CCTV recordings/images from An Garda Síochána will be formally recorded. If a law enforcement authority, such as An Garda Síochána, is seeking a recording for a specific investigation, An Garda Síochána may require a warrant and accordingly any such request made by An Garda Síochána should be requested in writing and the Institute will seek legal advice if deemed necessary.

4.4 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Institute, including the Student Handbook, Staff Handbook, the Anti Bullying and Harassment Policy and all other relevant policies and guidelines.

4.5 This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

4.6 CCTV monitoring of public areas for security purposes within the Institute premises is limited to uses that do not violate the individual’s reasonable expectation to privacy.

4.7 CCTV systems will not be used to monitor normal lecturer/student academic activity, or normal activity of any other staff.

4.8 All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the Institute. Recognisable images captured by CCTV systems are “personal data.” They are therefore subject to the provisions of the Data Protection Act 2018 (Ireland) and for the purpose of the General Data Protection Regulations (GDPR) EU 2016/679.

4.9 The CCTV system may be used to support contractors undertaking works or services on campus as an additional security measure. System(s) will provide coverage of a works site within the campus boundary if practicable, to act as a deterrent to potential criminal activity and to protect the Contractors equipment, materials, site accommodation, site storage etc. Contractor’s staff personal data will be treated and managed strictly in accordance with this policy and GDPR. Generally works sites on campus are part of existing facilities or in the immediate vicinity of a campus facility and therefore the comprehensive protection of these sites enables the Institutes to meets its obligations under security and the provision of a safe and secure environment for students, staff, visitors and Contractors.

5. **Justification for Use of CCTV**

5.1 Part 5 Chapter 2 S71 (1)(c) of the Data Protection Act 2018 (Ireland) requires that data is "adequate, relevant and not excessive" for the purpose for which it is processed. This means that the Institute needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The use of CCTV for security purposes has been deemed to be necessary by the Executive Management Team.

5.2 In areas of the premises where CCTV has been installed, e.g. hallways, stairwells, public spaces, the Institute has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that it is fair to assume may arise – See Appendix A – Privacy Risk Assessment.
6. Location of Cameras

6.1 The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy will not be permitted. The Institute has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. 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.

6.2 CCTV Video Monitoring and Recording of Public Areas in Athlone Institute of Technology may include the following:

5.2.1 Campus grounds: The Campus (Main and East) boundaries, main vehicular and pedestrian entrances, roadways, car parks, footpaths and paved areas, soft and hard landscaped areas.

5.2.2 Institute buildings and property: The Campus building stock; perimeters, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services

7. Surveillance and Criminal Investigation

7.1 The Institute will not engage in covert surveillance.

7.2 Where An Garda Síochána requests to carry out covert surveillance on Institute premises, such covert surveillance may require the consent of a judge and the approval of the President of the Institute or his nominee. Accordingly, any such request made by An Garda Síochána will be requested in writing and the Institute will seek legal advice.

7.3 CCTV will be used for:

7.3.1 Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas.

7.3.2 Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms.

7.3.3 Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control.

7.3.4 Criminal Investigations (carried out by An Garda Síochána): Robbery, burglary, criminal damage and theft surveillance

8. Notification - Signage

8.1 The Institute will provide a copy of this CCTV Policy on request to staff, students, and visitors to the Campus. This policy describes the purpose and general location of CCTV monitoring, contact details for those wishing to discuss CCTV monitoring and guidelines for its use. The location of CCTV cameras will also be advised to Executive Management. Adequate signage will be placed at appropriate locations, around the Institute, to indicate that CCTV is in operation. This CCTV Policy document will be available on the AIT website and on request from the Estates Office.

Figure 1: Sample Sign
8.2 Appropriate locations for signage will include:

- At entrance points to campus
- Main entrances to buildings
- Other locations with high footfall

9. **Data and Storage Retention**

9.1 Part 5 Chapter 2 S71 (1)(e) of the Data Protection Act 2018 (Ireland) states that data "the data shall be kept in a form that permits the identification of a data subject for no longer than is necessary for the purposes for which the data are processed". 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 (30 days), except where the images identify an issue – such as a break-in, theft, or injury to person/s, and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

9.1.1 Accordingly, the images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

9.2 The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised Estates personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Estates Manager. The Estates Manager may delegate the administration of the CCTV System to another staff member. Such delegation must be in writing. See Point 10.8 for access protocol around establishing identity or other facts. The names of authorised personnel will be advised to the Information and Compliance Officer.

9.3 CCTV Footage/images 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. A sample of the log of access is included in Appendix C.

9.4 CCTV footage of an incident that occurs on campus will be held for a period of two years to comply with the statute of limitations for persons making a personal injury claim. When the Institute becomes aware of the issue the person(s) involved in the incident will be informed in writing, that the footage is available to them and that a copy is going to be retained by the Institute. The footage will be erased at the end of the statutory period, except where the Institute has been informed by a party that an injury/illness has occurred.

9.5 The Institute reserves the right to retain footage of an incident indefinitely in situations where there is a reasonable expectation that an exemption to the statute of limitations may occur. The decision to retain footage will be communicated in writing to the person(s) involved in the incident.

10. **Access**

10.1 Devices storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. The area will be locked when not occupied by authorised personnel. A log of access to footage/images will be maintained (refer to Appendix C).

10.2 Access to the CCTV system and stored images will be restricted to authorised personnel only i.e. Estates Manager or delegated person.
10.3 In relevant circumstances, CCTV footage may be accessed:

10.3.1 By An Garda Síochána where the Institute (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
10.3.2 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 Institute property, or
10.3.3 By the HSE and/or any other statutory body charged with child safeguarding; or
10.3.4 To assist the Institute in establishing facts in cases of unacceptable behaviour.
10.3.5 Where data subjects (or their legal representatives), submit an access request where the time, date and location of the recordings is furnished to the Institute or
10.3.6 By individuals (or their legal representatives) subject to a court order.
10.3.7 For the Institutes insurance company where the insurance company requires same in order to:
   10.3.7.1 Pursue a claim for damage done to the insured property.
   10.3.7.2 Establish the facts of a personal injury claim.
10.3.8 By Contractors; where there has been a security or other issue on a campus site or related area

10.4 Requests by An Garda Síochána. On receipt of a written request for CCTV footage, by An Garda Síochána, to assist in the investigation of a criminal matter, the Institute will provide a copy of the footage requested, if available. For practical purposes, and to expedite a request in urgent situations, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request. There is a distinction between a request by An Garda Síochána to view CCTV footage and to download copies of CCTV footage. In general, An Garda Síochána making a request to simply view footage on the premises of a data controller or processor would not raise any specific concerns from a data protection perspective.

10.5 Data Subject 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 Information Compliance Officer at:
Information and Compliance Office
Athlone Institute of Technology
Dublin Road
Athlone
Co. Westmeath
dp@ait.ie
090 6468009

10.5.1 The Institute will respond within 30 days. Due to the size of the Institutes premises, the number of campus occupants, requests for personal footage or images must not be spurious or vexatious in nature.
10.5.2 The person making the request should provide the Institute with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the location, approximate time and the specific date(s) on which their image was recorded. It is not sufficient to make a submission requesting a copy of all CCTV footage held containing their personal data - it is necessary to specify that they are seeking a copy of all CCTV footage in relation to them which was recorded on a specific date between certain hours at a specific location.

10.5.3 Requesters should be aware that if the request is beyond 30 days from the date of footage is captured the recording no longer exists and it will not be possible to get access to a copy.

10.5.4 Where 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 the Institute is not obliged to supply the footage.

10.5.5 Images of other individuals will be obscured before the data is released. The format in which the data is provided will be decided by the Institute.

10.6 General requests. All other requests for footage from the CCTV systems must be made in writing by the person seeking the footage by fully completing the CCTV Footage Access Request Form (see Appendix B) and submitting to the Estates Manager.

10.7 CCTV footage will only be viewed (and provided if necessary) in compliance with the conditions of this policy. If the request is in conflict with this policy, footage will not be made available to view and will not be provided.

10.8 Establishing Person(s) Identity or other facts. On occasion, it may be necessary to request the assistance of a third party to identify person(s) on CCTV footage or to establish the facts of an incident. Where this is necessary the rationale for involving a third party will be recorded by the Estates Manager.

10.8.1 The Estates Manager will ensure that any person requested to view CCTV footage for the purposes listed in 10.8 above will sign a confidentiality agreement (reference Appendix D).

11. Responsibilities of the Estates Manager

11.1 Ensure that the use of CCTV system is implemented in accordance with the policy set down by the Institute

11.2 Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the Institute

11.3 Ensure that all existing CCTV monitoring system will be evaluated for compliance with this policy

11.4 Ensure that the CCTV monitoring at the Institute is consistent with best practice

11.5 Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy

11.6 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

11.7 Ensure that monitoring recorded tapes are not duplicated for release unless such an action is in compliance with this policy.

11.8 Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally

11.9 Approve the location of temporary security cameras to be used during special events that have particular security requirements and ensure their removal following such events.

11.10 Respond to complaints/appeals and advise on the Institute appeals process (Appendix F)
11.11 Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the Institute and be mindful that no such infringement is likely to take place.

11.12 Co-operate with the Health & Safety Officer of the Institute in reporting on the CCTV system in operation in the Institute.

11.13 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”.

11.14 Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only.

11.15 Ensure compliance as per Section 8 of this policy.

11.16 Ensure that the CCTV systems are operated in accordance with this policy.

12. Security Companies and Data Protection

12.1 The Institute CCTV system will be maintained by a third party security company contracted by the Institute.

12.2 Security companies that place and operate cameras on behalf of clients are considered to be "Data Processors." As data processors, they operate under the instruction of data controllers (their clients). The GDPR 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 and 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.

12.3 Any Security company or companies contracted by the Institute to install, operate, maintain and service CCTV systems must hold valid and applicable PSA Licenses.

13. Implementation & Review

13.1 The policy will be reviewed and evaluated annually. On-going review and evaluation will take cognisance of changing information or guidelines (e.g. from the Data Protection Commissioner, An Garda Síochána, Department of Education and Skills, Audit units (internal and external to the Institute) the C&AG, national management bodies, legislation and feedback from students, staff and others.

13.2 The date from which the policy will apply is the date of adoption by the Executive Management Team as noted on the front of this document. Implementation of the policy will be monitored by the Estates Manager, Data Protection Officer and designated personnel.