CCTV Policy

Owner: Facilities Manager
Issue Date: October 2018
Review Date: August 2019

Annexes

A CCTV System time check
B Request for CCTV Training
C Training Log
D Authorised Data Users
E Incident Log
F Request for Observations
G Internal Viewing Record
H Third Party Viewing
I Evidence Receipt
J Data Destruction Record
K Fault Log

Introduction

1 This policy sets out the principles and purpose of the CCTV system installed at Colchester Institute (CI). The standards set herein will be set as a minimum for all staff and authorised personnel to adhere to. It is the responsibility of the Facilities Manager to ensure that this document is available for reference on the College portal and is read and understood by the staff located at the location where the CCTV system is installed.

2. This CCTV policy should be read in conjunction with the CI Data Protection Policy, found on the CI portal and the Information Commissioners Office (ICO) CCTV - Code of Practice - Draft.

Ownership of Colchester Institute CCTV

3. The CCTV system is installed at the following locations:

a. Colchester Institute, Sheepen Rd, Colchester, Essex, CO3 3LL
b. The College at Clacton, Church Road, Clacton-on-Sea, CO15 6JQ
c. The College at Braintree, Church Lane, Braintree, CM7 5SN
d. The Learning Shop, 171a High Street, Dovercourt, CO12 3QB
e. Energy Skills Centre, Hamilton House, Foster Rd, Parkeston, Harwich, CO12 4QA.
f. The Minories, 74 High Street, Colchester, Essex, CO1 1UE.

The CCTV equipment located at a, b, c and d can be view centrally at Colchester Institute. The remaining are stand alone systems. Images are stored on hard drives for a period of 30 days.

The Data Controller is the: Facilities Manager. Tel: 01206 712111

The CCTV system is registered with the Information Commissioners Office (ICO) under registration number: Z4951392. Expiry date: 10 Aug 19.

Purpose of Colchester Institute CCTV

4. The CCTV systems are installed to support the business operations of Colchester Institute. Camera systems are installed both internally and externally for the purpose of enhancing the security of the buildings and equipment as well as creating a safe and secure environment for staff, students and visitors. CCTV is intended for the purposes of:

    a. Promoting a safer environment for staff, students, contractors and visitors.
    b. The reduction of graffiti, vandalism and other criminal damage.
    c. Detecting, preventing or reducing the incidence of property crime and offences against the person.
    d. Preventing and assisting with the resolution of cases of internal discipline.
    e. Preventing and reducing the risk of theft within the areas covered by the CCTV system.
    f. Preventing and responding effectively to other incidents that may arise during the course of our operations (eg harassment).
    g. Reviewing exam procedures within specialist environments.

Responsibilities

5. The Facilities Manager has overall responsibility for the management of CI CCTV system and ensuring that this policy and the CCTV - Code of Practice issued by the ICO are complied with.

6. The Security and Estates Manager is responsible for:

    a. ensuring that the CCTV system is registered with the ICO for the uses that it is employed for.

    b. Ensuring that any additional systems upgraded to the current CCTV equipment are registered.

    c. The day to day management of the CCTV system. This will include reviewing footage in the event of a security incident, controlling authorised maintenance and proposition of installation of new CCTV equipment.

7. The Data Protection Officer (DPO) is responsible for providing advice to the Facilities Manager on the disclosure of material in response to subject access requests. In accordance with the Data Protection Policy, the Data Controllers are responsible for handling Subject Access Requests and Complaints from Data Subjects.

8. Any Authorised Person who is responsible for operating the CCTV equipment in the absence of the Security and Estates Manager must be suitably trained, competent and where relevant licensed to operate the equipment. Training on the operation of the CCTV systems will be conducted by a suitably trained individual and this will normally be the Security and Estates Manager.

9. All staff should be aware of how to handle subject access requests or to whom such requests should be referred.

10. Any unauthorised staff member who accesses or tampers with the CCTV system without permission may face disciplinary action under the Colchester Institute Discipline Policy for Staff.

Stand Alone CCTV Equipment

11. College Management including Area Heads are responsible for compliance with this policy concerning any stand-alone CCTV equipment that is installed within their area; advice and guidance should be sought from the Security and Estates Manager on all aspects of CCTV use.

Storing and Viewing Surveillance Information

12. All images from CCTV systems are digitally stored on a designated computer hard drives, this method allows the authorised user to search the database when required, it is not possible to tamper with or alter any of the images.

13. In the event of the Police requiring CCTV images they can be uploaded onto a DVD/CD or an external hard drive, on receipt of the appropriate authorisation.

14. All CCTV images are held on the hard drive for a maximum of 30 days, if needed, images can be held longer subject to authorisation from the College Principal in the event of an ongoing security investigation.

15. The viewing of live images is controlled by the Security and Estates Manager, the CCTV monitoring equipment is secured in the Security and Estates office. When this office is empty it is always left secured. Stand alone CCTV equipment must be secured when not in use in order to deny unauthorised access.

Applications for Disclosure of Images

16. Individuals whose information is recorded have the right to view this information. Requests by individual data subjects for images relating to themselves, known as "Data Subject Access Request" should be submitted in writing to the appropriate Data Controller. The request should be confirmed in writing and any information held should be made available to them with 30 days of their request. Any request should be accompanied with the following information:

    a. Time, date and location of incident.
    b. Description of what they were wearing at the time.
    c. Photographic identification.

17. Third parties may request images if needed for an ongoing investigation, in relation to the prevention or detection of crime or in other circumstances where an exemption applies under relevant legislation. All requests by third parties should be made in writing to the appropriate Data Controller.

18. Any evidence that has been handed over to an authorised user must be accounted for, the evidence should be downloaded to an encrypted memory stick. The images on the memory stick should then be uploaded to the digital investigation folder on

the College Portal, the memory stick should then be returned to the Security and Estates Manager who will ensure that the images are deleted. The images on the digital investigation folder will then form part of evidence and will fall under the College Data Protection Policy.

Signage

19. Appropriate signage will be maintained at main entrances and at other locations where CCTV is in use, stating that CCTV is operating in this area. It is the responsibility of the Security and Estates Manager to ensure that CCTV signage complies with the ICO Code of Practice.

Complaints Procedure

20. All complaints concerning CI use of the CCTV system or the disclosure of images should be made in writing to the Security and Estates Manager. Appeals against the decisions of the Security and Estates Manager should be made in writing to the Facilities Manager. Receipt of the complaint letter should be returned within 10 working days of receiving a complaint, the Security and Estates Manager then has 30 days to deal with the complaint.

CCTV Policy Review

21. The Facilities Manager is responsible for reviewing the information contained within this CCTV policy including the annexes. The review will take place:

    a. Annually.
    b. On publication of new Acts, Regulations Approved Codes of Practice or Official Guidance.
    c. After any major CCTV upgrade.

Annex A to
CCTV Policy
Dated 13 Oct 18

System Time Check

Time check on the CCTV systems should be carried out on a weekly basis using an reliable means. If the system needs to be reset this needs to be noted in the column marked 'reset'.

Date	Time	Method Checked	CCTV ID	Reset	Name	Signature

Annex B to
CCTV Policy
Dated 13 Oct 18

Request for Training

All requests for CCTV related training are to be logged on this sheet and retained.

Requested by	Department	Line Manager	Date of Request	Dated Trained	Trained by

Annex C to
CCTV Policy
Dated 13 Oct 18

CCTV Trained Personnel Log

All staff who have received training on the CCTV equipment must sign this log, in signing this for you are stating that you have read the and understand the CCTV Policy, accompanying CCTV Regulations, GDPR and the Colchester Institute Data Protection Policy.

Date	Name	Department	Trained by	Signature	Notes

Annex D to
CCTV Policy
Dated 13 Oct 18

Authorised Data Processors

A Data Processor is any person authorised to view recordings or view CCTV monitors, this includes visiting service engineers. It is a criminal offence to allow access to recordings or the ability to view the CCTV to unauthorized persons.

Authorised Person	Authorised by	Business Name	Position	Signed	Date

Annex E to
CCTV Policy
Dated13 Oct 18

CCTV Incident Log

Record all incidents concerning the CCTV equipment on this form, this includes breakdowns, damages, vandalism etc.						
Location	**Camera No**	**Disc URN**	**Incident Details**	**Recorded by**	**Action taken**	**Date**

Request for Observation

Warning, if a request is made by the police or other public body in order to target a known individual or group of individuals, then written authority is requested under the Regulation of Investigatory Powers Act 2000 (RIPSA 2000 in Scotland). Local Authorities (Councils) have no power to target individuals inside dwellings or vehicle. Breach of RIP and RISPA is a criminal offence. Written authorization is not required if the police are in pursuit of a suspect which would make obtaining permission impracticable.

Date	Time	Person Requesting	Details of Request	RIPA Authority	Authorised by

Internal Viewing Record

Any specific activities that are viewed for a definite purpose by authorised persons shall be recorded here.

Date	Time	Incident Details	Reason Viewed	Viewed by	Authorised by

Third Party Viewing

Access to the CCTV data will be limited to those parties in the Authorised Data Processors Log. Any such access must be recorded in this form.

Date	Time	Entity of 3rd Party Disclosure	Reason for Disclosure	Extent of Access/Disclosure	Sign for Data Controller

Annex I to
CCTV Policy
Dated 13 Oct 18

Evidence Receipt

All evidence removed from the CCTV hard drive needs to be recorded here.

Date of request	Reference No	Details of incident (DTG)	Evidence handed over to	Signature	Return date	Signature

Annex J to
CCTV Policy
Dater 13 Oct 18

Data Destruction Log

All data requested for investigation purposes will be time sensitive, at the end of the agreed period of time all CCTV images are to be destroyed and the action recorded on this log.

Reference No	Date of destruction	Destroyed by	Signature	Remarks

Fault Log

Describe the fault in as much detail as possible, along with any related effects of the problem. This form should be passed to the person responsible for the CCTV system or your line manager. Use only one sheet per fault.				
Date	**Time**	**Nature of fault**	**Reported by**	**Engineer required**
Date	**Time**	**Fault rectified – Summary**	**Engineer**	**Docket Number**