CCTV Policy

Owner:	Security Manager
CE Sponsor:	EVP: Finance and Corporate Development
Issue Date:	August 2021
Review Date:	August 2024
Approval date:	August 2021

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 Security 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.

Related Policies

2. Data Protection Policy

Ownership of Colchester Institute CCTV

3. The CCTV system operated by Colchester Institute is installed at the following locations:

a. Colchester Institute, Sheepen Rd, Colchester, Essex, CO3 3LL
b. Braintree Campus, Church Lane, Braintree, CM7 5SN
c. The Learning Shop, 171a High Street, Dovercourt, CO 3QB
d. Energy Skills Centre, Hamilton House, Foster Rd, Parkeston, Harwich, CO12 4QA.

The CCTV equipment can be viewed centrally and images are stored on system hard drive for a period of 30 days.

Books for recording request for CCTV training, authorised data processors, CCTV incident log, viewing log, and fault log are all held and are available to be completed in the Security Managers office by the CCTV viewing area.

The Data Controller is the Security Manager: Tel: 01206 712057

The CCTV system is registered with the Information Commissioners Office (ICO) under registration number: Z4951392.

CCTV owned by others on Colchester Institute premises

4. Other CCTV system owned and operated by others on Colchester Institute premises include:

Location	Data Controller
AM2 Testing Centre	Head of Area, Mechanical and Electrical Services
Examinations Suite, The Learning Shops	Learning Shop Manager

These systems are governed by the policies held by the CCTV owners (examinations bodies). The Data Controllers shall be responsible for ensuring compliance with these policies, and for holding evidence of such in the event of inspection. Contact Data Controllers for more information.

5. 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 safeguarding 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.
g. Reviewing exam procedures within specialist environments.

Responsibilities

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

7. The Security 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.

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

9. Any Authorised Person who is responsible for operating the CCTV equipment in the absence of the Security 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 organisation who is SIA recognised.

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

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

Stand Alone CCTV Equipment

12. Nominated CLMG members are responsible for compliance with thispolicy and CCTV owner policy concerning any third party CCTV equipment that is installed within their area; advice and guidance can be sought from the Security Manager if required.

Storing and Viewing Surveillance Information

13. 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.

14. In the event of the Police requiring CCTV images they can be uploaded onto an external hard drive, on receipt of the appropriate authorisation.

15. 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.

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

Applications for Disclosure of Images

17. 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 informationheld 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.

18. 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.

19. 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 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

20. 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 Manger to ensure that CCTV signage complies with the ICO Code of Practice.

Complaints Procedure

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

CCTV Policy Review

22. The Security Manager is responsible for reviewing the information contained within this CCTV policy including the annexes. The review will take place:
    a) Every three years
    b) On publication of new Acts, Regulations, approved Codes of Practice or Official Guidance
    c) After any major CCTV upgrade