HUGHES HALL
UNIVERSITY OF CAMBRIDGE

CLOSED CIRCUIT TELEVISION (CCTV) POLICY AND PROCEDURES

1. INTRODUCTION

1.1 The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Hughes Hall, Cambridge. Cameras are used to monitor activities within College buildings, on its site, in its car parks and in other public areas, to identify criminal activity actually occurring, anticipated or perceived.

Cameras are also used for the purpose of securing the safety and well-being of the College, together with its Fellows, staff, students and visitors.

All viewings and copying of the CCTV footage will be documented and in compliance with current data protection legislation.

1.2 CCTV monitoring and recording systems will only be installed in or on College property when this has been reviewed and approved by the Head of Facilities.

1.3 The system comprises a number of fixed and fully functional cameras located in buildings and externally around the College site. These are monitored by appropriate personnel. The audio settings of the cameras are always switched off (except by permission, see 3.2.6)

1.4 This policy document will be subject to review biennially to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the College.

1.6 Independently installed and operated CCTV systems by Senior Members, staff or students will not be permitted on any College property and where found action will be taken to close these systems down.

2. OBJECTIVES OF THE CCTV POLICY

2.1 The objectives of the CCTV Policy are to:

(a) protect College property

(b) ensure a safer environment within the College

(c) assist in the investigation of suspected breaches of College regulations by staff or students

(d) support the Police in a bid to deter and detect crime, by providing evidence in support of an enquiry or prosecution

3. OPERATION OF THE CCTV SYSTEM

3.1 MANAGEMENT OF SYSTEM:

3.1.1 The CCTV operating system will be administered and managed by the Head of Facilities in accordance with the principles and objectives expressed in the College policy document.

3.1.2 The day-to-day management will be the responsibility of both the Head Porter during the working week and by the Duty Porter outside normal working hours and at weekends.

3.1.3 All cameras are monitored by authorised personnel, on the computers located within the Porters' Lodge, the Maintenance Manager's computer and the IT Manager's computer, by use of the CCTV system's software programme, which is installed and maintained by the College IT Department.

3.1.4 The CCTV system will be operated 24 hours a day, 365 days of the year.

3.1.5 Warning signs informing of the use of a CCTV system, as required by the Code of Practice of the Information Commissioner, will be placed at all access routes to areas covered by the College's CCTV cameras.

3.2 SYSTEM CONTROL - MONITORING PROCEDURES:

3.2.1 On a daily basis a member of the Porters' Lodge will check and confirm the efficiency of the system, ensuring that:

- The cameras are functional
- The equipment is properly recording

The Porters, Head Porter, Maintenance Manager and IT Manager are able to review the footage for monitoring purposes using the CCTV system's software programme installed on their PCs.

3.2.2 Management access to the CCTV System is strictly limited to the Head of Facilities, Head Porter, the Duty Porter, Maintenance Manager and IT Manager.

Any request to view the CCTV by any other person must be authorised by the Bursar.

Review and storage of pre-recorded footage (for longer than the 28 days specified in 3.4.1) is only possible if the event has been exported to an external storage device and is limited to the device it is exported to. All users of the system can perform this export function, but the only personnel authorised to export events are the Bursar, Maintenance Manager, IT Manager and Head Porter.

Storage (via exporting an event) is only permissible during internal or official investigations and is deleted when the investigation is complete.

3.2.3 The Porters' Lodge will only be staffed by departmental staff that are trained in the system's use and familiar with this policy.

3.2.4 There should always be at least one member of the Porters' Lodge present to actively monitor the system and the computer must be locked if unattended.

3.2.5 Personnel may not adjust the physical camera position or impede the viewing range of a camera without an authorization being obtained from the Bursar, Dean (or investigative officer instructed by the Dean), Head of Facilities or the Head Porter for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.2.6 The audio settings are to be kept switched off. Personnel may not switch on the audio settings without written permission from the Bursar or Senior Tutor.

3.2.7 If covert surveillance is planned or has taken place, copies of the written authorization, including any Review or Cancellation, must be returned to the Head of Facilities or their nominated Deputy.

Covert recording will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorised activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

3.2.8 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
Recording is carried out on digital data apparatus which is part of the College's IT system.

3.2.9 Recorded data will only be released for use in the investigation of a specific crime and with the written authority of the police. Any internal College review of recorded data during incident investigations must follow the authorisation process (see 3.2.2).

3.3 EXEMPTIONS:

3.3.1 The CCTV system is designed to ensure maximum effectiveness and efficiency, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.4 RETENTION AND DISPOSAL OF MATERIAL:

3.4.1 Footage will be stored internally per camera for a maximum of 28 days after which the system automatically deletes the footage. The exception to this retention rule is footage stored pending an internal or official investigation. The storage of footage is limited to authorised staff (see 3.2.2) and deleted when the investigation is complete.

4. <u>DIGITAL RECORDING PROCEDURES</u>

4.1 RULES FOR RETENTION OF DATA

4.1.1 In order to maintain and preserve the integrity of the events recorded on the CCTV cameras and the facility to use them in any future proceedings, the following procedures for their use and retention of data must be strictly adhered to:

4.1.2 Footage required for evidential purposes can be released to the police or other authorised third party on production of a signed data access request form and positive ID such as Police Warrant Card, Picture ID Card, Driver License. It will be provided on a suitable storage medium and will carry the date and time range of the footage.

4.1.3 The authorised person providing the footage will notify the Compliance Administrator and this will be recorded in the Compliance Log.

4.1.4 The exported file is readable by the majority of computer systems and should not require a specific CCTV data and viewer programme.

4.2 DEALING WITH OFFICIAL REQUESTS: USE OF CCTV IN RELATION TO CRIMIMAL INVESTIGATIONS AND INTERNAL INVESTIGATIONS:

4.2.1 CCTV recorded images may be viewed by the Police for the prevention and detection of crime, and by authorised officers of Hughes Hall (see 3.2.2) for supervisory or disciplinary purposes, authorised demonstration and training.

4.2.2 A record will be maintained in the Compliance Log of the release of Data to the Police or other authorised applicants.

4.2.3 Viewing of CCTV images by the Police, or any other authorized person must be recorded in writing and recorded in the Compliance Log. This will be under the management of the Head Porter**.** Information logged should include: name of person viewing image, time and date of viewing, time and date of images reviewed, brief reason for viewing content (e.g. “incident in corridor”) but should not contain names of individuals featured in the recording.

Except where requests fall under the terms of a pertinent Information Sharing Agreement, police requests to view CCTV footage will only be granted following correct process as dictated by the prevailing legislation at the pertinent period in time. For the avoidance of doubt this will be, as a minimum, a request in writing providing a detailed reasoning for the requirement, which is then to be authorized and facilitated by the Head Porter.

4.2.4 Should an export of the footage be required as evidence, a copy may be released to the Police under the procedures described in paragraph 4.1.2 of this Code.

4.2.5 Applications received from outside bodies (e.g. solicitors or insurance firms) to view or release footage will be referred to the Bursar. Footage will only be released where satisfactory documentary evidence is produced, showing that it is required for legal proceedings, or needs to be provided in response to a Court Order. A fee can be charged in such circumstances.

Footage will only be released to the Police or other outside bodies on the clear understanding that it remains the property of the College, and the information contained on it are to be treated in accordance with this policy.

The College retains the right to refuse permission for the Police or other outside bodies to pass the footage to any other person.

4.2.6 The Police may require the College to retain the footage for possible use as evidence in the future. Such footage will be properly indexed and securely stored under the management of the Head Porter until it is needed by the Police or other outside bodies.

Where a suspicion of misconduct arises and at the formal request of the Dean, HR Manager or another Investigating Officer, the Bursar may provide access to CCTV images for use in staff or student disciplinary cases.

5. BREACHES OF THE POLICY (INCLUDING BREACHES OF SECURITY)

5.1 Any suspected breach of the Policy will be initially investigated by the Head Porter or their nominated deputy, in order for them to take the appropriate action.

5.2 Where a breach of the Policy is identified by the Head Porter following their investigation an independent investigation will be conducted by an individual appointed by the Bursar, which will result in a detailed report with recommendations for action. This process will be overseen by the Bursar.

6. ASSESSMENT OF THE SCHEME

6.1 Performance monitoring, including random operating checks, may be carried out by the Head Porter or their nominated deputy.

7. COMPLAINTS

7.1 Any complaints about the College's CCTV system should be addressed to the Head Porter, Hughes Hall, Cambridge CB1 2EW.

7.2 Complaints will be investigated in accordance with Section 5 of this policy.

8. ACCESS BY THE DATA SUBJECT

8.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to access data held about themselves, including that obtained by CCTV.

8.2 Requests for Data Subject access should be made on a Subject Access Request form, available from the Compliance Administrator.

8.3 Where the College is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

For further information, please contact:

Head Porter, Hughes Hall, Cambridge, CB1 2EW.

9. PUBLIC INFORMATION

Copies of the College's CCTV Policy are publicly available from the Head Porter.

This document was reviewed February 2021 and is next due for review February 2023.

Signed: ……

Jonathan Horwood, Head of Facilities

Date: ……

Appendix 1 - Checklist for users of CCTV systems monitoring premises

This CCTV system and the images produced by it are controlled by the Head of Facilities, who is responsible for how the system is used. We have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of residents and visitors. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

	Checked (Date)	By	Date of next review
The annual Data Protection Fee has been paid to the ICO, requirement for use of CCTV has been reviewed and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, with access only by a limited number of authorised persons.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to any external third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals requesting copies of their own images, and if unsure the controller knows to seek advice from the Compliance Administrator.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Please keep this checklist in a safe place until the date of the next review.