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. Cameras are used to monitor activities within College buildings, on its site, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived.
Also 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 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 (Pan/Tilt/Zoom) cameras located in buildings and externally around the College site.
These are monitored by appropriate personnel.

1.4 The CCTV policy will be registered with the Information Commissioner

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

1.6 The CCTV system is owned by the College.

1.7 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) 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 Porter 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 'on call' duty Porter outside normal working hours and at weekends.

3.1.3 All cameras are monitored by authorised personal on computers within the Porters' Lodge by use of the 'Mobotix' programme 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, 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.

3.1.6 Liaison meetings may be held with all bodies involved in the support of the system.

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.

3.2.2 Access to the CCTV System will be strictly limited to the Bursar, Senior Tutor, Head of Facilities, Head Porter, Out-of-Hours Duty Persons and the Duty Porters.

Other departments/persons requiring access to the CCTV system are as follows:-

The Head of Domestic Operations will be allowed access to the CCTV system which covers the Bar and till areas.
The Librarian will be allowed access to the CCTV system which covers all areas within the Libraries.
The Archives Team will be allowed access to the CCTV system covering all areas within the Archives.
Un-authorized persons are not permitted to view live or pre-recorded footage.
Any request to view the CCTV by any other person must be authorised by the Bursar, Senior Tutor or the Head of Facilities.

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

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

3.2.5 Unless an immediate response to events is required, Porters must not re- direct cameras at an individual, their property or a specific group of individuals, without an authorization being obtained from the Bursar, Senior Tutor,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 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.

3.2.7 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

3.2.8 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 to the media for use in the investigation of a specific crime and with the written authority of the police. Recorded data will never be released to the media for purposes of entertainment.

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 Data disks will be disposed of after 3 months by a secure method.

3.4.2 Footage will be stored on the hard drive for 14 days with the exception of the Archives footage when it will be stored for one month.

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 Digital Video Recorder (DVR) Hard Disks used to record events from 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 Each DVR must be identified by a unique mark or serial number. This will be recorded in a log book managed by the Head Porter.

4.1.3 Each DVR must be kept in a secure location with access restricted to authorised staff.

4.1.4 A disk required for evidential purposes must be of the CD-R type only, disks will be provided in pairs each carrying an identical identification number, one a Master Disk to be retained by the College, the other a Copy which can be released to the police or other authorised third party on production of a signed data access request form.

4.1.5 The disk should be loaded with the required CCTV data and viewer programme; identical information should be loaded on both Master and Copy disks.

4.1.6 Each disk should be sealed in its own case; the Master Copy should be kept in a secure storage area. The Copy disk is handed to the person making the request on

production of positive ID such as Police Warrant Card, Picture ID Card, Driver License, etc.,

4.1.7 The record sheet should then be completed and the Copy disk signed for and counter signed by the authorised person, (Duty Porter).

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

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

4.2.2 A record will be maintained of the release of Data on Disk to the Police or other authorised applicants. A register will be available for this purpose.

4.2.3 Viewing of CCTV images by the Police, or any other authorized person must be recorded in writing and entered in the logbook. This will be under the management of the Head Porter**.**
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 a disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 4.1.4 of this Code.
Disks will only be released to the Police on the clear understanding that the disk remains the property of the College, and both the disk and information contained on it are to be treated in accordance with this policy.

4.2.5 The College retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained therein.

4.2.6 The Police may require the College to retain the stored disk(s) for possible use as evidence in the future. Such disk(s) will be properly indexed and securely stored under the management of the Head Porter until they are needed by the Police.

4.2.7 Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Head Porter. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order. A fee can be charged in such circumstances.

5. <u>BREACHES OF THE POLICY (INCLUDING BREACHES OF SECURITY)</u>

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 an application form.

For further information, please contact:

Head Porter
Hughes Hall, Cambridge
CB1 2EW.

9. PUBLIC INFORMATION

Copies of the College's CCTV Policy will be available to the public from the Head Porter.

This document was reviewed in May 2018 and is due to be reviewed again in May 2020.

Signed: …….

Jonathan Aveling, Head Porter

Date: 23 May 2018

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 and for notifying the Information Commissioner about the CCTV system and its purpose.

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
Notification has been submitted to the Information Commissioner 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, where only a limited number of authorised persons may have access to them.			

The recorded images will only be retained long enough for any incident to come to light (eg for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to 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 making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
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.