

CCTV Policy and Procedures

Introduction

The purpose of this Policy is to regulate the management, operation and use of the Closed Circuit Television (CCTV) system at Clare Hall ('the College'). Cameras are used to monitor activities within College buildings, on its sites, its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the College, together with its Fellows, staff, students and visitors.

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

The system comprises a number of fixed and fully functional (Pan/Tilt/Zoom) cameras located in buildings and externally around the College's grounds. These are monitored by appropriate personnel.

The CCTV policy will be registered with the Information Commissioner under the terms of the General Data Protection Regulation (GDPR). The College's use of CCTV complies with the requirements of the GDPR and, where applicable, the Regulation of Investigatory Powers Act 2000.

The CCTV system is owned by the College.

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

Objectives of the CCTV Policy

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.

Operation of the CCTV System

Management of the system

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.

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

All cameras are monitored by the Porter in the Porters' Lodge

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

Emergency procedures will be used when it becomes necessary to call the Emergency Services.

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.

System control - Monitoring procedures:

On a daily basis a member of the Porters' Lodge will check and confirm:

- the cameras are functional
- the equipment is properly recording

Access to the CCTV System will be strictly limited to the Duty Porters and specific authorised persons. Unauthorised persons are not permitted to view live or pre-recorded footage.

The Porters' Lodge will only be staffed by those who are trained in the system's use and familiar with the policy.

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

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 authorisation being obtained from the Head Porter for directed surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

If covert surveillance is planned or has taken place, copies of the written authorisation, including any review or cancellation, must be returned to the Bursar or nominated deputy.

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. These are controlled by the IT technicians of the College.

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.

Exemptions:

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.

Retention and disposal of material:

Data storage devices will be disposed of by a secure method.

Footage will be stored on data recorder hard drives for up to 28 days.

Footage will only be stored on data storage devices if footage is requested by external agencies in the process of detecting crime and in the prosecution of offenders.

Digital Recording Procedures

Rules for retention of data

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:

Each DVR must be identified by a unique mark or number. This is maintained by the Head Porter.

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

A recording required for evidential purposes must be provided in pairs each carrying an identical identification number, one a master recording 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.

The recording should be loaded with the required CCTV data and viewer programme; identical information should be loaded on both master and copy devices.

The master copy should be kept in a secure storage drawer. The copy device is handed to the person making the request on production of positive ID such as Police Warrant Card, picture ID Card, Driving Licence, etc.

The record sheet should then be completed and the copy disk signed for and counter signed by the Duty Porter

Dealing with official requests: use of CCTV in relation to criminal investigations:

CCTV recorded images may be viewed by the Police for the prevention and detection of crime, and authorised members of the College for supervisory purposes, discipline reasons or authorised demonstration and training.

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.

Viewing of CCTV images by the Police must be recorded in writing and entered in the log book. This will be under the management of the Head Porter. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

Should a recording be required as evidence, a copy may be released to the Police under the procedures described in paragraph 4.1.3 of this Code. Recordings will only be released to the Police on the clear understanding that the recording remains the property of the College, and both the device and information contained on it are to be treated in accordance with this policy.

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.

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

Applications received from outside bodies (e.g. solicitors) to view or release disks will be referred to the Bursar. In these circumstances recordings 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.

Breaches of the Policy (including Breaches of Security)

Any breach of the Policy by the Porters or other authorised staff will be initially investigated by the Head Porter or his nominated deputy, in order for him/her to initiate the appropriate disciplinary action.

Any serious breach of the policy will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Assessment of the Scheme

Performance monitoring, including random operating checks, may be carried out by the Head Porter or his/her nominated deputy.

Complaints

Any complaints about the College's CCTV system should be addressed to the Bursar, Clare Hall, Herschel Road, Cambridge, CB3 9AL.

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

Access by the Data Subject

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.

Requests for Data Subject access should be made in writing to the Bursar, following the Subject Access Request Policy.

For further information, please contact:

The Bursar
Clare Hall
Herschel Road
Cambridge
CB3 9AL