CHURCHILL COLLEGE
CAMBRIDGE CB3 0DS

CCTV Policy

Policy Name	CCTV Policy
Purpose	The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Churchill College.
Owner	Facilities Manager/Head Porter
Contact	Head Porter
Approved By	
Approval Date	
Next Review Due	July 2025
Version and Recent Changes	Composed 2014, revised 2018. Reviewed 2022, Updated version approved 16 July 2024.

CCTV Policy

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 Churchill College. 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 Director of Estates and Operations.

1.3 The system comprises of fixed and fully functional (pan/tilt/zoom) cameras located in buildings and externally around the College site. These are passively monitored by appropriate personnel.

1.4 The CCTV policy will be registered with the Information Commissioner. The College's use of CCTV complies with the requirements of current data protection legislation: (http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cctvfinal_2301.pdf) and where applicable, the Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents

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 staff/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 CCTC 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 the 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 'Milestone X Protect Smart Client' 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 If out-of-hours emergency maintenance is required, the duty Porter must contact the out-of-hours College IT Department for assistance.

3.1.6 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.

3.1.7 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, and the equipment is properly recording.

3.2.2 Access to the CCTV System will be strictly limited to the Senior Tutor, Bursar, Head Porter, Estates and Operations Director, HR and Governance Director Facilities Manager and the Duty Porters. Other departments/persons requiring access to the CCTV system are as follows:

- The Head of Catering 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 Senior Management Team will be allowed access to the CCTV system covering all areas within the Archives.
- The AV Department will be allowed access to live coverage of the CCTV system covering conference areas to aid with Customer support.
- The Facilities, Operations and Centre Management teams at the Moller Institute will be allowed access to live coverage of CCTV Pole C only.
- The HR and Governance Director will be allowed to request CCTV recordings where

suspected staff misconduct is being investigated and relevant footage may be viewed by the appointed Investigating Officer and may be used as evidence in disciplinary proceedings.

- Unauthorised 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 Head Porter, Senior Tutor or the Director of Estates and Operations.

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 when required 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 Senior Tutor, Director of Estates and Operations 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 Director of Estates and Operations 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.

3.4.3 All digital recordings should be password protected and retained for one month after any investigation has been completed, when the file will be deleted.

4. Digital Recording Procedures

4.1 Rules of the 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 logbook 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, (Porter).

4.2 Dealing with Official Requests/Use of CCTV in Relation to Criminal and Disciplinary Investigations

4.2.1 CCTV recorded images may be viewed by the Police for the prevention and detection of crime. Authorised officers of Churchill College may also view images for supervisory purposes, demonstration, training.

4.2.2 CCTV recordings may be viewed by authorised personnel for the purposes of conducting disciplinary investigations and may be used in disciplinary proceedings where CCTV evidence tends to show, in the reasonable belief of the College, that there is a disciplinary case to answer for misconduct. The individual will be given a chance to see and respond to the images in these circumstances.

4.2.3 CCTV will not be operated in toilets, private offices or changing rooms, unless this is necessary for the investigation of a serious crime or there are circumstances in which there is a serious risk to health and safety or to the operation of the employer's business. CCTV will be used in this way only where it is a proportionate means of achieving the aim in the circumstances.

4.2.4 Covert CCTV will only ever be set up for the investigation or detection of crime or serious

misconduct. The use of covert CCTV will be justified only in circumstances where the investigator has a reasonable suspicion that the crime or serious misconduct is taking place and where CCTV use is likely to be a proportionate means of securing evidence. Any covert recording will be strictly time limited.

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

4.2.6 Viewing of CCTV images by the Police, or any other authorised 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 authorised and facilitated by the Head Porter.

4.2.7 Should a disk or electronic copy 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 and or electronic copy will only be released to the Police on the clear understanding that the disk/electronic copy remains the property of the College, and both the disk/electronic copy and information contained on it are to be treated in accordance with this policy.

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

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

4.2.10 Applications received from outside bodies (e.g. solicitors) to view or release disks/electronic copies will be referred to the Head Porter. In these circumstances, disks/electronic copies 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. Breaches of this 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 a Head of Department, appointed by the HR Manager, which will result in a detailed report with recommendations for action. This process will be overseen by the HR Manager or a person nominated by them.

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, Churchill College, Storey's Way Cambridge CB3 0DS. 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. Requests for Data Subject access should be made on an application form, which is available at https://www.chu.cam.ac.uk/about/official-documents/data-protection-resources/.

9. Public Information

9.1 Copies of the College's CCTV Policy will be available to the public from the Head Porter and on the College website (https://www.chu.cam.ac.uk/about/official-documents/).

Reviewed 3/6/24
Next review: 07.2025
Reviewed by Paolo Paschalis, Facilities Manager and Hannah James (College Data Protection Lead)
Reviewed 3rd June 2024