CCTV POLICY AND CODE OF PRACTICE

Introduction

The purpose of this Policy and Code of Practice is to ensure that the College uses CCTV responsibly and with effective safeguards. The intention is:

1. To create a safer working environment for staff and students in the College.
2. To protect property belonging to the College, its students and staff.
3. To provide evidence in support of any internal or external enquiry, disciplinary proceedings or prosecution, especially if associated with the security of the College site and members of the College community, criminal activity committed on College property, or the misuse of College property or equipment.

The cameras should not face into College buildings, except where agreed in advance with student representatives via the College's Consultative Committee except in exceptional circumstances. Cameras stream video to dedicated CCTV servers, from where they can be viewed on a real time basis in the Porter's Lodge, Library, and other approved locations. Recordings are made onto the hard disks of the CCTV servers for replay in the event of an incident.

This Policy and Code of Practice sets out the appropriate actions and procedures, which must be followed to comply with the relevant data protection legislation in respect of the use of CCTV surveillance systems managed by the College. This policy and code of conduct intends:

1. To inform all who come onto the College site that CCTV is in use.
2. To keep CCTV data secure and controlled by authorised personnel.
3. To maintain all CCTV equipment in working order.
4. To provide retention of CCTV data within the stated purpose only.
5. To state the manner and means of destroying stored CCTV data.
6. To prevent access by unauthorised individuals or third parties.

Responsibilities

The system is operated by the College and is in use all year round. The Bursar has overall responsibility for the implementation and use of the system. The IT Director and IT department ensures all equipment is maintained and in a suitable condition. The Porters, Library Staff, IT staff, and other College Officers will interrogate the system and its data. Operation of the system is restricted to those named above.

Staff who use the CCTV system have the following responsibilities:

1. To uphold the arrangements of this Policy and Code of Practice.
2. To handle CCTV data securely and responsibly, within the aims of the Policy and Code of Practice.
3. To be aware that they could be committing a criminal offence if they misuse CCTV data.
4. To report any breach of procedure to the Bursar or College Data Protection Lead.
5. To attend training / refresher sessions as required.

Siting the Cameras

Prior to any camera installation the Bursar and the College Data Protection Lead will ensure that the installation complies with the relevant data protection legislation and the CCTV Policy and Code of Practice. It is essential that the location of the equipment is carefully considered; the way in which CCTV captures data will need to consider the privacy of all individuals. All camera locations are visible to public and staff. Signs have been erected at the main entrance to notify all those who enter that they are entering an area that is covered by CCTV cameras.

Processing CCTV data for an in-progress incident

The following procedures concern the viewing and use of the CCTV data in response to an in-progress incident in the College.

1. The Porters, Library staff and IT staff may directly view the live feeds from any camera during their working hours.
2. In response to an in-progress incident the above staff may view recently recorded data to ascertain facts necessary to respond to the event.
3. No recordings or copies of CCTV data is permitted; if this is necessary then the following policy for processing CCTV data for past incidents must be followed.

Processing CCTV data for past incidents

The following procedures concerning the use and retention of recordings should be followed to provide an acceptable level of security and accountability, and to ensure the acceptance of recordings in support of criminal proceedings.

1. Recordings for most cameras are retained on the CCTV server for up to 30 days and are then overwritten.
2. Recordings for cameras covering long term student storage areas (trunk stores, etc.) are retained on the CCTV server for up to 90 days and are then overwritten.
3. Requests for the retention and/or disclosure of CCTV material should be made to the Head Porter and be recorded on the CCTV Request form (Appendix A).
4. The Head Porter may view or authorise a Porter to view past recordings stored on the service to establish if the CCTV system has recorded images relevant to a request for disclosure or retention, and for this reason alone. All viewings of recordings, and the reason for viewing, must be logged in the CCTV Log held by the Head Porter.
5. If it appears that relevant material is held and that CCTV recordings need retaining or disclosing permission must be sought from two authorised College Officers, or one authorised College Officer and the Head Porter. Authorised College Officers in this regard are the College Data Protection Lead, the College Proctor, the Senior Tutor and the Bursar. As part of this process authorised College Officers may view the CCTV material in question.

6. Once a valid request has been made the IT department will process the footage and generate a master copy of the recording.
7. A copy of the relevant part of the recordings will be stored on digital media. The CCTV request form should be held with the digital media in a secure format and handed to the Head Porter immediately.
8. The Head Porter, or a nominated deputy, should mark each item of digital media with a unique reference number.
9. All digital media will be securely stored by the Head Porter until they are no longer needed by the college, are passed to the Police or are passed to a third party with approval of the College Data Protection Lead.
10. The IT Department is responsible for destroying all digital copies when they are no longer needed for evidence. Digital copies should be destroyed, by appropriate means for the specific media and disposed of in the confidential waste container. Each disposal should be noted in the CCTV Log.
11. The Head Porter, or a nominated deputy, is responsible for ensuring that the CCTV log is kept up to date.

Access to and Disclosure of CCTV data to Third Parties

Access to, and disclosure of, CCTV data is restricted and carefully controlled to ensure privacy of individuals, but also to ensure that the continuity of evidence remains intact should the data be required for evidential purposes.

IT staff need access to CCTV data for maintaining the CCTV system. Individuals requesting access to CCTV data should complete a CCTV Request form (Appendix A). Any request by a third party to view a CCTV recording **must be approved** by the College Data Protection Lead in consultation with the Bursar, who will determine whether disclosure is necessary, legitimate and lawful. All unsuccessful requests will be retained for 3 months.

Once this has been actioned the details should be recorded in the CCTV Log held by the Head Porter. Any digital media that is requested by the Police in connection with a criminal enquiry will be released against an Officer's signature and the completion of CCTV Request form (Appendix A), after authorisation by the Bursar in connection with staff matters and by the Senior Tutor in respect of students.

Any individual wishing to make a subject access request is asked to review the Colleges Data Protection policy at http://www.pem.cam.ac.uk/the-college/legal-information/data-protection/.

On no account may CCTV data be viewed by any unauthorised person, or removed from the College without the specific approval of the Senior Tutor, College Data Protection Lead, Bursar or Head Porter. Staff will be informed that any misuse or unauthorised access of live CCTV data will be considered as a serious disciplinary matter.

If the College is asked to retain a recording for evidential purposes, the Head Porter will take possession and securely store the relevant digital media for as long as is required, which would normally be until one month after the finalisation of any court proceedings.

Complaints Procedure

Any individual who has concerns about the CCTV system or the control of it at Pembroke College is requested to write to the Bursar or the College Data Protection Lead outlining the reason for the complaint.

Information and Training

A copy of this Policy and Code of Practice will be published also in the Staff Handbook.

All Porters will be trained in the practical use of the CCTV system. The Head Porter, Senior Porters and IT Personnel will receive additional training in the storage, capture and recording of CCTV data. The Bursar, Head Porter, Senior Porters and IT Staff will be issued with a copy of the Information Commissioner's CCTV Code of Practice.

Implementation, Monitoring and Review of this Policy

This policy will take effect from May 2021. The H&S Officer has overall responsibility for implementing and monitoring this policy, which will be reviewed on a regular basis following its implementation (at least annually) and additionally whenever there are relevant changes in legislation or to our working practices.

APPENDIX A

REQUEST ID:

PEMBROKE COLLEGE - CAMBRIDGE

1. REQUESTERS PERSONAL DETAILS	
Applicant's full name:	Applicant's postal address:
Applicant's email address:	

2. INFORMATION REQUIRED	
To help us find the CCTV data you require, please complete the following section.	
Location/position of CCTV camera:	Date and time of incident:
Brief description of the incident to be retrieved, the appearance of any individuals and likely activities captured by CCTV: **Please give all information that might assist us in finding the incident**	
Purpose of the request: (e.g. Subject Access Request / Evidence for investigation / Police Request / Disciplinary) **If the purpose of the request is a subject access request ensure the College Data Protection Lead is consulted, for all other requests consult the Bursar.**	

3. WORKFLOW *(Office Use Only)*	
Name/Role of Approvers:	Approval status (Confirmed/Denied):
Name/Role of individual consulting CCTV record:	Date Copies Made:
Digital Media Reference Number('s):	
Digital Media Destruction Date:	Digital Media Destruction Actioned By:
Name of recipient('s):	Organisation of Recipient('s):
Badge Number of Recipient('s): **Optional – If digital media is being released to the Police service**	Purpose of release: