CHRIST'S COLLEGE
UNIVERSITY OF CAMBRIDGE

Closed Circuit Television (CCTV) Policy

Introduction

Christ's College operates a Closed-Circuit Television (CCTV) system to provide a safe environment for students, staff and visitors while also protecting College property.

This document details the accepted use and administration of the CCTV system, and the images captured on it to ensure the College complies with the GDPR, Data Protection Act and other relevant legislation.

This policy was created in line with the Code of Practice dated June 2017 v1.2, issued by the Information Commissioners Office and since updated with additional information available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/.

Purpose

The College has installed the CCTV system with the main aim of reducing the threat of crime, protecting College property and ensuring the safety of all individuals. In order to accomplish this objective, the system has the following purposes:

1. Deter individuals who may have criminal intent
2. Assist with the prevention and detection of crime
3. Assist with the identification, apprehension and prosecution of offenders in relation to criminal and public order offences
4. Assist with the identification of individuals, activities and incidents which may result in disciplinary proceedings against students, staff, contractors, volunteers or Fellows involved
5. Monitor the security of the site
6. Facilitate the movement and control of vehicles using the College car parks
7. Monitor the safety and security of College buildings
8. Enable the identification of individual(s) who misuse College property
9. Identify individuals who remove books from the Library without first using self-service checkout
10. Ensure the safety of lone users of the College Fitness Suite and pool area

Covert Recording

Covert cameras may only be used under the following circumstances and with the written authorisation of the Director of College Services or Bursar where it has been assessed by at least two Senior College Officers as being necessary because:

1. Informing the individual(s) concerned that the recording was taking place would seriously prejudice the objective of making the recording

2. There is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place (e.g. harassment or intimidation of a student)

Any such recording and subsequent processing:

1. Will be done in compliance with the Regulation of Investigatory Powers Act
2. Will only be done for a reasonable and limited period in keeping with the objective for the recording.
3. The covert recording will only relate to the specific suspected unauthorised or illegal activity.
4. The decision to initiate covert recording will be fully documented and will set out how the decision to record covertly was reached and by whom.

Cameras

- The College will position cameras to cover as much of the College premises as possible with particular emphasis on the entrances to the site.
- The College will make every effort to position the cameras so that they will only cover College property.
- The cameras will not focus on residential accommodation except for entranceways and public areas.
- The College will display clear signs to identify that individuals are entering an area that is under CCTV surveillance.
- Cameras will be sited in locations that protect them from being vandalised whilst still allowing them to provide images with the necessary quality and field of view.
- The quality of the image will be assessed on a routine basis, which is to be no longer than annually, to ensure they continue to provide the required standard. This procedure will be carried out in conjunction with the College's approved security contractor.
- The cameras will be correctly maintained and if broken will be repaired ASAP to ensure image quality is acceptable for the purpose for which it is intended. A log of all maintenance should be kept using the fault reporting system
- The cameras will not employ any audio recording mechanism. If a replacement camera is installed which has this capability this ability will be disabled.
- No camera capable of automatic facial recognition will be employed.

Retention

The images captured by the system will be saved for the current 24-hour period and a further thirty days will be kept in the archive. Any video older than the archive retention period will normally be deleted unless it constitutes evidence relating to a specific incident. The archive period will be reviewed annually to ensure it is appropriate, it will however also be reviewed as part of any post-incident review. The archive period will be the shortest amount of time required for the system to fulfil its purpose.

Staff

The images captured by the system will be monitored by the College Porters who are responsible for security. The Director of College Services has overall responsibility for the system, but operational responsibility belongs to the Head Porter.
The Duty Porters will monitor the system at their workstation. Their monitors are installed behind the main reception desk so that only they can view the images. The monitors will not be moved from this location and no unauthorised members of staff will be allowed access to the monitors.
Requests for image disclosure should be sent to the Head Porter or his deputy who will be able to review any image stored within the defined retention period. Only they or IT staff are able to download images.

IT staff and CCTV contractors will occasionally view images to ensure the system is working efficiently and to correct any faults that may occur.

All Porters will be briefed on the sensitivity of handling the video images and trained in the correct operation of the system.

Disclosure of images

The disclosure of images will be treated with care to ensure the rights of the individual(s) and fair processing. There may be rare circumstance when the release of images to a third party is required as their need outweighs those of the individual(s) whose image(s) were recorded.
Disclosure will be limited to:

1. Police and other law enforcement agencies, where the images could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
2. Prosecution agencies
3. Relevant legal representative
4. People whose images have been recorded and retained. This will not occur if such a disclosure will prejudice a criminal enquiry or proceedings
5. Member of College or University staff involved with a disciplinary process
6. In rare cases to others to assist in the identification of a perpetrator, witness or victim of a criminal incident (e.g. to provide an insurance company with evidence of damage occurring to a car in the car park)

All disclosures should be logged to include date, reason (including crime number if applicable), recipient, job function of the recipient and their organisation, reason, person who released it and details of the images released and what media was used.
The method used to provide the media should be secure (e.g. an unencrypted USB stick sent via standard post should not be used) and preferably by hand where the recipient can sign the Porters logbook to confirm their receipt.

Individual's access rights

The UK General Data Protection Regulation (GDPR) gives individuals the right to access personal information about themselves including CCTV images. All such requests should be referred to the Head Porter. The Head Porter or their deputy will liaise with the

Information Manager to ensure compliance, and that no third-party information is revealed. The individual will be asked to provide:

1. Date and Time
2. Location in College
3. Any additional information to allow identification of the individual's images (e.g. a photo and/or accurate description of clothing)

The Information Manager or Bursar as the College Data Protection Lead has the right to refuse the request especially if the release of the information would prejudice an on-going criminal or disciplinary case.
Individuals have the right to prevent processing of their images if such processing is likely to cause substantial and unwarranted damage to them. All such requests should still be made to the Head Porter who will consult with the Information Manager or the Bursar. The individual will be notified in writing of the outcome no later than 30 days from the receipt of the request.

Freedom of Information or EIR requests

The release of any personally identifiable information (PII) is exempt under the FOI or EIR as it must follow UK GDPR data principles; this includes the information held in this system.

This policy may be released under the Freedom of Information Act.

Complaints

Any complaints about the system should in the first instance be addressed by the Head Porter. If the complainant is not satisfied with the response received, they should write to the Director of College Services.
Any requests relating to the General Data Protection Regulation or Freedom of Information Act should be addressed to the College Compliance Office at the address below:

Christ's College
St Andrew's Street
Cambridge CB2 3BU
UK
For UK GDPR requests, email dpa@christs.cam.ac.uk or foi@christs.cam.ac.uk for FOI requests