



Policy responsibility: Domestic Bursar

Introduction

St John's College uses closed-circuit television (CCTV) to create a safe and secure environment and to protect its premises and property.

This policy sets out the parameters for the use of CCTV by the College. It takes account of the UK General Data Protection Regulation (GDPR), the Data Protection Act 2018, and guidance from the Home Office and from the Information Commissioner's Office. It should be read alongside the relevant Privacy Notice.

The Head Porter is responsible for the operation and management of the CCTV system. Enquiries about its use should be addressed to the Head Porter.

The Domestic Bursar is the responsible College Officer, and is responsible for authorising any use of covert recordings in accordance with Section 4 below.

Strategic decisions about the deployment of surveillance cameras on the College estate will be taken by the **College Council**.

1. Purposes of CCTV

The purposes of deploying CCTV are to:

- a) promote the safety and security of Fellows, students, staff and visitors;
- b) monitor and help ensure the security of the College's premises and property;
- c) assist in the prevention, detection and investigation of crime, and provide evidence for any subsequent prosecution;
- d) support investigations and provide evidence for external disciplinary proceedings by the University of Cambridge, any College, or any other relevant organisation;
- e) support the detection and investigation of any activity that might warrant internal actions or disciplinary proceedings, and assist in any subsequent proceedings;
- f) support investigations into and provide evidence about any accidents or incidents covered by health and safety legislation.

2. Cameras and locations

CCTV cameras are deployed at strategic locations throughout the College. Additional deployments of cameras will be considered where necessary and in line with the aims of this policy.

There is no coverage of private areas, including toilets, shower facilities, changing rooms, staff break rooms, private residential rooms or Fellows' rooms.

All cameras are positioned overtly so they are visible. The capture of images of people not on the premises will be minimised as far as is practical.

Signage should be displayed to inform the College community and the public that a surveillance camera system is in operation. Signs should be displayed at the main access points to make people aware that they are entering an area covered by CCTV.

3. Monitoring, recording and retention of images

CCTV Images are monitored by members of the Porters' team. Routine review and playback of recorded footage, in line with this policy, forms part of the Porters' role.

Two camera systems are in operation. Images are either recorded onto a secure drive or retained in a cloud system. Only authorised users have access to these systems.

Cameras provide high-quality, clear images so they are effective in fulfilling their intended purpose. Cameras are named and images are date- and time-stamped.

CCTV images will be retained for no longer than 30 days from the date of recording unless required for evidential purposes or the investigation of allegations. After that point images will be automatically overwritten.

If images are shared with an external third party, such as a law enforcement agency, in accordance with section 5 below, the third party will become the data controller of those images. The College keeps records of data sharing with third parties.

The Head Porter must authorise the retention of any image for longer than 30 days and is responsible for reviewing the continued necessity of that retention.

4. Access, copying and disclosure

Access to images is restricted to ensure the rights of individuals are protected and that the College remains compliant with data protection legislation. Images can be accessed or disclosed only where necessary to fulfil the purposes for which they were originally collected.

Only Porters who operate the system in the course of their duties, designated staff in the IT and Digital Services Department, and system managers can access live and recorded images.

All access to recorded images, other than routine use by the porters including within their digital systems, will be documented. Viewings of recorded images will take place in a restricted area, from which anyone not directly involved is excluded.

If any images are copied or transferred out of the system for viewing, then this will be documented. Access documentation will be reviewed annually to ensure appropriate use.

The Domestic Bursar, Head Porter and Deputy Head Porter are the only people who may permit other members or employees of the College to view images, in accordance with this Policy and with data protection legislation.

The following College personnel may request access to images:

- a) Heads of Department, when investigating allegations of staff misconduct or health and safety issues;
- b) The Dean of Student Discipline, Senior Tutor or Tutor for Postgraduates when investigating allegations of student misconduct or where a student may be at risk.

The Domestic Bursar, Head Porter and Deputy Head Porter are the only people who can authorise the viewing or disclosure of images to a third party.

Images will be disclosed to third parties in limited circumstances, and in accordance with the purposes for which the system is intended, including disclosure to:

- a) the police and other law enforcement agencies, where the recorded images could assist in the prevention or detection of crime;
- b) prosecution agencies, such as the Crown Prosecution Service;
- c) relevant legal representatives;

- d) another College, the University, or another relevant organisation, where a clear case has been made that the recorded images could assist in an investigation under their disciplinary procedures, where the disclosure is necessary for an investigation under the College's disciplinary procedures, or where sharing recordings support the purposes of CCTV deployment listed in Section 1;
- e) Third parties, such as solicitors, requiring CCTV evidence in legal proceedings.

All requests for disclosure or access to images will be documented. The record will include the reason access or disclosure was requested, the reason for allowing the request, the date of any disclosure or provision, the identity of the person or persons to whom the images were disclosed or provided, and the extent of the information disclosed or provided.

If disclosure or access was denied, the reason will be recorded.

5. Applications by data subjects

Under data protection legislation individuals have the right to request a copy of the personal data that the College holds about them. This includes images in which they are identifiable.

A written request should be made to the College Data Protection Lead (CDPL) at dataprotection@joh.cam.ac.uk. Requests should ideally include the date and time when the images were recorded and the location of the camera(s) from which images are sought.

The CDPL will determine whether disclosure is proportionate; if it would involve disclosing images of other parties or revealing information about another party; and whether it is necessary to redact images relating to them to avoid an unfair intrusion into their privacy.

If the College is unable to comply with a data access request within the time required by law, or because disclosure could prejudice the prevention or detection of crime, the apprehension or prosecution of offenders, or internal disciplinary proceedings, the applicant will be informed.

6. Compliance and complaints

The College will make sure that everyone handling surveillance camera images and recordings is trained in the operation and administration of the system, in the operation of this policy, and on the implications of data protection legislation for operation of the system.

They will also be made aware that they are only authorised to use the system in a way that is consistent with the purposes, aims and procedures outlined in this document.

Individuals are personally responsible for complying with this policy. Any deviation from it may constitute a breach of the College's Rules for the Use of IT Services or may amount to an offence under s.170 of the Data Protection Act 2018.

Any complaints concerning the use of or management of the College's CCTV system should be directed to the Head Porter.

Review schedule:	Annual factual update; three-yearly review Next full review date: 5 August 2029, with factual updates to be made every year on or near this date.
Reference:	SJC_POR_POL_001

APPENDIX 1: List of legislation, guidance and policies

The following legislation, guidance and policies are relevant to this policy:

UK GDPR: Defines the rights of European citizens in relation to the processing of their personal data. The UK GDPR represents the divergence of the UK from the EU GDPR following Brexit.

Data Protection Act 2018: Brings the EU's General Data Protection into UK law, including setting the rules for law enforcement processing.

ICO Video Surveillance Guidance: Advice from the UK's privacy regulator on the operation of video surveillance systems that view or record individuals.

Biometrics and Surveillance Camera Commissioner's Amended Code of Practice: This is not binding for a Cambridge College but the Home Office encourages voluntary adoption as a matter of good practice.

College Rules for the Use of IT Services: The College's IT acceptable use policy.
