

CODE OF PRACTICE 3

CCTV Policy

Contents

1. Introduction and Accountability	1
2. Closed Circuit Television.....	2
Objectives	2
Covert filming or monitoring	2
3A. Data Protection.....	2
3B. CCTC Guiding Principles.....	3
4. Administration	4
5. Storing and Viewing Images	5
6. Disclosure of images to third parties	5
7. Signage	6
8. Disclosure of images to the data subject (Subject Access Requests).....	6
9. Access to / Disclosure of CCTV.....	6

1. Introduction and Accountability

Following the Government’s commitment to further regulate Closed Circuit Television (CCTV), the Protection of Freedoms Act 2012 (PFA) provided for the development of a Code of Practice relating to CCTV and other surveillance camera systems, and the appointment of a Surveillance Camera Commissioner.

The ‘Surveillance Code of Practice’ pursuant to the Protection of Freedoms Act 2012 was published in August 2013. It will help ensure that a system operator makes transparent decisions about the legitimacy and proportionality of surveillance.

This Code of Practice covers the College’s CCTV and is intended to reflect the spirit and guidance issued by the Information Commissioner’s Office, as documented in the ‘Protection of Freedoms Act 2012’.

2. Closed Circuit Television

- a) City of London College ('The College') is the owner of public closed circuit television (CCTV) systems currently installed on its campuses and in/on College property off campus. The SMT at the College retains overall responsibility for the system and delegates the day to day management to IT Support team.
- b) All images produced by the system remain the property of the College.
- c) The vast majority of our cameras are overt, with the images recorded centrally, and are all viewable centrally by trained Staff. In addition, a limited number of management staff have the facility to monitor cameras sited within their own areas of responsibility. See also 'Covert filming or monitoring' section, below.
- d) The primary Security Control room is situated on the XXXX
- e) Unlawful access to the data and images is prevented by key access to secure areas, 24 hour manning, and controlled IT system login.

Objectives

Objectives of the CCTV Schemes:

To assist in providing a safe and secure environment for the benefit of those who might visit, work or live within the College's campuses. Subject to this Code of Practice the schemes will not be used to invade the privacy of any individual student, business or other private premises and enforcement.

The CCTV systems will only be used for the following purposes and within this Code of Practice.

- To reduce the fear of crime and to reassure students, staff and visitors.
- To deter and detect crime, public disorder and anti-social behaviour.
- To identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour.
- To provide the College with evidence upon which to take criminal and civil action.
- Staff and student discipline: The College will only use the images in a staff disciplinary case when there is suspicion of misconduct and not to generally monitor staff activity; likewise the images will only be used as evidence in serious student disciplinary cases being heard by the College Discipline Committee and or other higher authority.
- Upon formal request, to assist Police and other law enforcement agencies with the pursuit of their objectives.

Covert filming or monitoring:

Covert filming or monitoring may be used as part of a specific time-limited investigation where informing subjects of or signposting the activity would have a prejudicial effect on that investigation. The decision to use covert monitoring as a proactive investigation tactic may only be taken after consultation with the DPO in their absence and with written authorisation from the SMT. Covert monitoring shall only be used for the prevention and detection of criminal activity or equivalent malpractice.

3A. Data Protection

1. The College is committed to complying with the requirements of the General Data Protection Regulation (GDPR) and intends to operate the system in accordance with the data protection principles set out in the GDPR.
2. The standards, which must be met if the requirements of the GDPR are to be satisfied, are based on the data protection principles set out in Article 5 of the GDPR which are:
 1. personal data shall be processed lawfully, fairly and in a transparent manner;
 2. personal data shall be collected for specified, explicit and legitimate purposes only, and will not be processed in a way that is incompatible with those legitimate purposes;
 3. only personal data that is adequate, relevant and necessary for the relevant purposes shall be processed;
 4. personal data must be accurate and must be kept up to date; reasonable steps must be taken to ensure that inaccurate personal data are deleted or corrected without delay;
 5. personal data can be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and
 6. appropriate technical and organisational measures must be taken to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The College (as controller in most cases where it processes personal data) is also responsible to demonstrate compliance with the above data protection principles.

All members of staff involved in operating the system will be made aware of the objectives of the scheme and will be permitted only to use the system to achieve those objectives.

3B. CCTC Guiding Principles

The College has adopted the following 12 guiding principles of the Code:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.”
The College recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of staff should be aware of the restrictions relating to this set out in this Code and the rights of individuals under the GDPR and the Surveillance Camera Code of Practice (SCCoP) as published by the Surveillance Camera Commissioner. **More information:** www.gov.uk/surveillance-camera-commissioner

4. Administration

CCTV:

- a) It is the responsibility of the SMT (or IT Support team) to:
 - Select camera sites and initial areas to be viewed.
 - Be responsible for compliance with the GDPR and SCCoP.
 - Take responsibility for control of the images and make decisions on how these can be used.
 - Ensure the system is secure and only viewed by authorised personnel.
 - Ensure that the procedures of this Code of Practice comply with the current data Protection law and SCCoP.
 - Introduce a CCTV incident log and record of Police or other Statutory Authority requests for images.
 - Ensure adequate signage is erected.
 - Regularly evaluate the system and its usage to ensure it continues to comply with the latest legislation, CCTV Codes of Practice.
- b) It is the responsibility of the IT Support team to:
 - Clearly communicate the specific purposes of the recording of and use of images and objectives to all staff in duty.

- Ensure that a CCTV incident log and record of Police or other Statutory Authority requests for images is maintained.
- Carry out audit checks at 6 monthly intervals (at a minimum) to check that procedures are being correctly followed. Records of audits to be kept.

5. Storing and Viewing Images

- a) All images recorded on the College's CCTV cameras are digitally stored on computer/server hard drives, and although the images can be searched, it is not possible to tamper or alter them.
- b) In the event of the Police requiring CCTV images they can be 'burnt' onto a CD/DVD for evidence in court, on receipt of the appropriate Data Protection form.
- c) The CCTV images over record after 30 days, however any relevant images can be locked on the hard drive for future reference. All retained images are subject to the controls outlined in these procedures.
- d) Viewing of live images on monitors is restricted to IT Support operators and other authorised personnel and can only be accessed using passwords.
- e) Images are viewed in confidence in secure private offices.
- f) Requests to view images or image disclosure of third parties should be made in writing to the DPO and SMT.

6. Disclosure of images to third parties

- a) The following guidelines will be adhered to in relation to disclosure of images:
 - Will be in line with the objectives (see 3B above) • Will be controlled under the supervision of the SMT.
 - A log book/sheet will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for disclosure
 - The appropriate disclosure documentation from the Police will be attached to the log entry
 - Images **must not** be forwarded to the media or be placed on the internet or otherwise distributed without specific and written prior approval of the Board of Governors acting in compliance with the law and these procedures. Failure to comply will result in disciplinary action being taken. Images will only be released to the media for legitimate purposes (e.g. identification of data subjects) and in liaison with the Police or other law enforcement agency.
- b) Any other requests for images should be routed via the SMT, as disclosure of these may be unfair or unlawful to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of individuals whose images are recorded.
- c) The College has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body such as the Police, then they become the data controller for their copy of that image. It is their responsibility to comply with the GDPR in relation to any further disclosures.

7. Signage

Signage has been erected at the main entrances to the College campuses and at other locations where CCTV is in use, stating that CCTV is in operation.

It is the responsibility of the SMT and IT Support Team to ensure that adequate signage is erected to comply with the Information Commissioner's Code of Practice.

8. Disclosure of images to the data subject (Subject Access Requests)

Individuals whose images are recorded have a right to view the images of themselves, or their vehicles and, unless they agree otherwise, to be provided with a copy of the images. All such requests are handled by the College's Data Protection Officer in liaison with SMT and IT Support Team.

- Images must be provided within 40 calendar days of the request being received.
- Those who request access must provide proof of identity and details which allow the College to identify them as the subject of the images and to assist with locating the relevant image(s) on the system.
 - - A log of such requests will be maintained.
 - - If images of third parties are also shown within the requested images of the person who has made the access request, consideration must be given as to whether there is a need to obscure the images of the third parties.

9. Access to / Disclosure of CCTV

The College respects the right of individuals to check the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system.

Document Custodian: Senior Management Team
Review Cycle: Annually, or as required in response to regulatory or strategic changes
Last Reviewed: August 2025
Effective Date: August 2025
Review Date: August 2026
Version: 1.8.25
Circulation: Public: (Web Publication)
Sensitivity: Unclassified