South Thames Colleges Group

CCTV Policy

Introduction

The South Thames Colleges Group (the Group) is committed to operating a safe environment for its students, staff and others than visit Group premises.

To support this commitment the Group operates closed-circuit television ("CCTV") system at each campus to promote safety, prevent and detect crime, reduce vandalism and to protect Colleges Group property.

CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under the Data Protection Act. As such, all CCTV activity is managed in accordance with the Data Protection Act 2018, UK GDPR, the Protection of Freedoms Act 2012, the Surveillance Camera Code of Practice, and the Information Commissioner's CCTV Code of Practice.

The system comprises a number of fixed and dome cameras located both internally and externally at each campus. Cameras are not routinely monitored live, and access to recordings is strictly controlled and limited to authorised personnel.

The CCTV system is owned and operated by the Group and its operation will be subject to review on an annual basis.

The purpose of this Policy is to regulate the management, operation and use of the CCTV system at across the Group. This document sets out the accepted use and management of the CCTV system and images to ensure the College complies with the Data Protection Act, The Protection of Freedoms Act, The Surveillance Camera Code of Practice and other relevant legislation.

The College has produced this policy in line with the current Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

Purpose of CCTV

The South Thames Colleges Group has installed CCTV systems to:

- Protect College buildings and its assets to ensure they are kept free from intrusion, vandalism, damage or disruption
- To increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation and crime.
- To support the Police in in the investigation of offences and in a bid to deter and detect crime.
- Assist with the identification, apprehension and prosecution of offenders.
- Support disciplinary investigations involving staff, students or other users of the premises where appropriate.
- Assist with the effective management and security of the College buildings on a day-to-day basis.
- Provide management information relating to Contract Compliance of 3rd party service providers.
- Monitor vehicle movement and safety around campus areas.

Prevent and deter serious vandalism, criminal damage and anti-social behaviour in identified high-risk areas, including restricted coverage within communal areas of toilet facilities, where justified and authorised in accordance with this Policy.

The CCTV system will be provided and operated in a way that is consistent with an individual's right to privacy.

*Must be read alongside - Appendix 1 – Evidence of damaged toilets, Additional cameras list & DIPA.

Overview of System

The CCTV system runs 24 hours a day, 7 days a week but images are recorded on most devices when motion is detected, therefore recordings will not be continuous. The CCTV system comprises fixed position cameras; pan tilt and zoom cameras; monitors; multiplexers; digital recorders and public information signs.

CCTV cameras are located at strategic points at each campus, principally at the entrance and exit point for the site and various buildings, as well as main thoroughfares throughout the site.

CCTV signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use, its purpose and details of the operator.

Although every effort has been made to ensure maximum effectiveness of the CCTV system; it does not cover all areas and it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

CCTV in Toilets and Sensitive Areas (Restricted Coverage)

In exceptional circumstances, CCTV may be installed in toilet facilities where there is a demonstrable, ongoing and significant risk of serious vandalism, criminal damage, anti-social behaviour, or threats to safety, and where alternative control measures have been exhausted or proven ineffective.

The use of CCTV in such areas is subject to enhanced safeguards and strict limitations:

- CCTV cameras will not be installed within toilet cubicles, urinals, or any area where individuals have a reasonable expectation of complete privacy.
- Coverage is strictly limited to communal areas only, such as:
- Entrance and exit points
- Wash-hand basin areas
- Mirror, hand-dryer and circulation areas
- Cameras will be positioned and configured to avoid capturing intimate activity.
- CCTV in toilet areas will not be routinely monitored live.
- Recordings will only be accessed where an incident has occurred and where viewing is necessary and proportionate for investigation purposes.

CCTV installation in toilet areas will only take place following:

- Completion and approval of a Data Protection Impact Assessment (DPIA)
- Written authorisation from the Director of Facilities and the Director of Planning and Information
- Confirmation that appropriate and clear signage is in place

CCTV in toilet areas will never be used for monitoring personal behaviour, performance, or routine activity.

Operation

The Director of Facilities is responsible for ensuring the CCTV facilities are used in accordance with this policy and that the system is fully operational. The Head of Facilities with the locally based Facilities Manager for each site is responsible for the day-to-day operation of the system and ensuring compliance with this policy.

The Security staff will hold an SIA CCTV Licence. The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements both of the Data Protection Act 2018 and the Commissioner's Code of Practice.

CCTV will be used to monitor activities within each campus, the car parks and other Group owned areas for the purpose of securing the safety and wellbeing of the occupants within the College grounds, together with its visitors. Static cameras will not focus on private homes, gardens and other areas of private property. Operators of cameras with tilt and pan and zoom capability will not direct cameras at an individual, their property or a specific group of individuals, without verbal authorisation as required in accordance with this policy.

Information or images secured as a result of CCTV system will not be used for commercial purpose. They will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. CCTV images will never be released to the media for purposes of entertainment.

The planning and design of the existing CCTV system has endeavoured to ensure that the CCTV system will give maximum effectiveness and efficiency but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at access routes and areas covered by the college CCTV System.

Image Viewing and Download Procedure

CCTV Recordings may be viewed by and provided to the Police if the request and the authorisation by the Director of Facilities, or in their absence the Head of Facilities provided the request is made in accordance with the Group procedures for the release of personal staff or student information to the Police.

CCTV recordings of staff that are deemed to be necessary to investigate an allegation of misconduct by a member staff may be viewed and provided by the Deputy CEO or in their absence the Director of HR where:

- There is a dispute over the events in respect of the allegation that CCTV may assist in resolving
- The member of staff concerned have been told that the review of CCTV will be taking place before the viewing and any down load takes place

CCTV recordings of students or other users of a Group site that are deemed to be necessary to investigate an allegation of misconduct may be viewed and provided by a select group of individuals who are trained, these are the Deputy CEO, Director of Facilities, Executive Principles , Director of Student Services and Group Security Manager where:

- There is a dispute over the events in respect of the allegation that CCTV may assist in resolving
- The student(s) or user(s) concerned have been told that the review of CCTV will be taking place before the viewing and any down load takes place

Should a download be required as evidence, an electronic copy may only be made by a holder of a SIA CCTV Licence. All requests for downloads will be retained by the Site Facilities Manager for 12 months or after the incident that the download relates to has been closed.

Covert Recording

Covert recording of staff, students or other uses of Group premises is only authorised in exceptional circumstances.

Prior to authorisation for covert recording to take place the applicant must have demonstrated and documented that other procedures and practices were not sufficient to prevent or detect suspected illegal or unauthorised activity from taking place. Any approved covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.
The decision to adopt covert recording will be made by the Deputy CEO or in their absence the Director of HR in the case of staff, the Director of Student Services, in the case of students and the Director of Facilities for other users. Any approval will be fully documented and will set out how the decision to use covert recording was reached and by whom. Covert recording may be used under the following circumstances:

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording.
- That there is reasonable cause to suspect that illegal activity is taking place or is about to take place or unauthorised activity is taking place; that may seriously or substantially affect the operation or reputation of the Group.

Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 31 days from the date of recording. A record of data destruction will be made in confirmation on the authorised request to make covert recordings.

The system will not be used to:

- Provide images to the world wide web
- Recordsound
- Disclose to the media

Breaches of this Policy

Any suspected breach of this Policy by College staff will be considered under the Group Disciplinary Policy and Procedures.

Data Protection Act

For the purpose of the Data Protection Act 2018, South Thames Colleges Group is the data controller.

- CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act 2018. This policy is consistent with the Group's Data Protection Policy, the provisions of which should be adhered to at all times.
- The Group has registered its processing of personal data (including CCTV) with the Information Commissioner's Office (ICO).

Where new cameras are to be installed on Group premises, Part 4 of the ICO's CCTV Code of Practice will be followed before installation:

- The appropriateness of and reasons for using CCTV will be assessed and documented;
- The purpose of the proposed CCTV system will be established and documented;
- Responsibility for day-to-day compliance with this policy will be established and documented;

Individual Access Rights

The Data Protection Act gives individuals the right to access personal information about themselves, including CCTV images.

All requests for access to view/copy CCTV footage by individuals should be made in writing to the Director of Planning and Information

Requests for access to CCTV images must include:

- The reason for the request
- The date and time the images were recorded
- Information to identify the individual, if necessary
- The location of the CCTV camera
- Proof of Identity

The Group will respond promptly and at the latest within 30 calendar days of receiving the request processing fee, determined by the Director of Facilities and sufficient information to identify the images requested. If the College cannot comply with the request, the reasons will be documented. The requester will be advised of these in writing, where possible.

Access to Images by Third Parties

Unlike Data Subjects, third parties who wish to have a copy of CCTV images (i.e. images not of the person making the request) do not have a right of access to images under the DPA, and care must be taken when complying with such requests to ensure that neither the DPA, HRA or the CCTV Policy are breached. As noted above, requests from third parties will only be granted if the requestor satisfies the following criteria:

- Prosecution agencies and their Legal Representatives
- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry)
- Insurance Companies and their Legal Representatives

All third party requests for access to a copy of CCTV footage should be made in writing to the Director of Planning and Information. A law enforcement or prosecution agency requesting access they should make a request under Section 29 of the Data Protection Act 1998.

Retention and Disposal:

CCTV Recorded images will be retained for no longer than 31 days from the date of recording, unless required for evidential purposes or the investigation of crime or otherwise required and retained as a download with the requisite approval form.

All images on electronic storage will be erased by automated system overwriting. All downloads, still photographs and hard copy prints will be securely disposed of as confidential waste. The date and method of destruction will be recorded on the bottom of the original approval to copy held by the Group Head of Security.

Central Responsibilities:

- The Director of Planning and Information is consulted on the Policy to ensure compliance with GDPR.
- The SLT is responsible for approving this Policy.
- The Director of Facilities is responsible for compliance with, and the implementation of procedures to comply with this policy.

Complaints:

Complaints regarding the CCTV system and its operation should be made under the Group complaints procedure.

Forms for Use with this Policy:

- Request to carry out Covert Recording
- CCTV Data Release Form

South Thames Colleges Group

Request to carry out Covert Recording

To: Facilities Manager
Authorised by: Principal/Deputy Principal ☐
Reason for Request: **Location:**
Length of Time required:

Date Requested:
Requested By:
Signature:

Facilities Manager to confirm data has been disposed of:		
Date:	**Method of Destruction:**	
Signed:	**Print Name:**	**Date:**

South Thames Colleges Group

Request to view / download CCTV / produce evidence (Non-Police)

Type of request for images relating to: Staff ☐ Student ☐ Public ☐ **Reason(s) for viewing / copying / downloading/ Production of CCTV – tick below** College Group internal detection of crime ☐ Student disciplinary investigation ☐ HR investigation ☐ Subject Access Request ☐
Incident Date/Time/Precise location / Names (if known) and brief description of required incident- Please include descriptions of those you seek to identify within CCTV:
Name of person making request: **<u>Please note that by signing this you are agreeing to comply with South Thames College Group CCTV and Security Policy:</u>** **Date:** **Signature:** **Print Name:**
Authorised by: **If your request relates to staff:** Director of HR ☐ or Deputy CEO ☐
If your request relates to student: Deputy CEO ☐ or Director of Facilities ☐
If your request relates to Individual Access Rights: Director of Planning and Information ☐ or Deputy CEO ☐

Signed:	**Print Name:**	**Date:**