CCTV Code of Practice

1. Introduction

The aim of this code of practice is to ensure that the closed circuit television system of St George's, University of London stands up to scrutiny and is accountable to the people it aims to protect.

The code of practice for St George's University closed circuit television (CCTV) systems, operated by contracted security services, is underpinned by the CCTV Code of Practice, Security Industry Authority (SIA) standards and Security's operations assignment instructions / procedures.

2. Scope

This code of practice applies to all employees, students and visitors of St George's, University of London and all employees of contracted services. This code does not apply to standalone webcams or cameras whose purpose is solely research or teaching.

3. Ownership and operation of the CCTV System

The CCTV system is operated by security personnel contracted to St George's, University of London. The CCTV and all recorded material is owned by St George's, University of London.

4. Principles

The following principles will govern the operation of the CCTV system:

1) The CCTV system will be operated fairly and lawfully and only for the purposes authorised by St George's, University of London
2) The CCTV system will be operated with due regard for privacy of the individual
3) Any changes to the purpose for which the CCTV system is operated will require the prior approval from the Director of Estates & Facilities and will be publicised in advance

5. Purpose of the CCTV system

The system is intended to assist in providing a safe and secure environment and an increased level of security in the University for the benefit of those who study, work, live in or visit the campus.

The objectives for the use of the CCTV systems, which will be subject to assessment on regular basis.

- To detect, prevent or reduce the incidence of crime
- To improve the operational response for security patrols in and around the areas where CCTV operates

- Create a safer community
- To gather evidence by a fair and accountable method
- To provide emergency services assistance
- To assist with health & safety
- To assist in the monitoring and deployment of security staff during emergency situations
- To investigate suspected breaches of university policy / regulations

As community confidence in the system is essential, an appropriate maintenance programme is in place.

System Details:

The CCTV system consists of overt cameras situated on university property, which continuously records activities in the area of coverage. The security control centre is staffed by qualified and Security Industry Authority (SIA) licenced staff. All systems record 24 hours a day.

6. Data protection legislation

Recorded images of living, identifiable individuals constitutes personal data under data protection legislation. The university is committed to complying with the requirements and will operate the system in accordance with the eight principles. Any changes to data protection legislation will be adhered to and any future changes of legislation will be taken into account.

7. Covert cameras

Use of covert cameras will only be authorised by the Principal in exceptional circumstances where there is reason to suspect criminal activity or a serious breach of university regulations and where notification of the monitoring would be likely to prejudice the prevention or detection of the activity. The period of monitoring will be as narrow as possible to allow the investigation off the alleged offence. Monitoring will desist when the investigation is complete.

8. Access to information

All visitors to the Security Control Centre will be required to read sign the visitors' book and a declaration of confidentiality regardless of their status.

Access to the Security Control Centre and recorded / live footage will be prohibited except for lawful, proper and sufficient reasons and this will be assessed on a case-by-case basis and only then on written / verbal authorisation from the Facilities Manager or the Customer Services Manager. Any such visits will be conducted and recorded in accordance with the assignment instructions / procedures.

As a public body the university may receive freedom of information requests under the Freedom of Information Act (FOIA). All such requests are dealt with centrally by the university's Governance, Legal & Assurance Services.

Section 40 of the FOIA contains a two-part exemption in relation to information about individuals. When a request for CCTV footage is received the following should be considered:

- Are the images those of the requester? If so, the information is exempt from the FOIA. Instead this request should be treated as a data protection subject access request.
- Are the images of other people? These can be disclosed if only if disclosing the information in question does not breach the data protection principals.

9. Request to view footage

All request to view CCTV footage will be dealt with in accordance to the Freedom of Information Act and Data Protection Legislation:

A Viewing Request Form is required to be completed, clearly setting out why the request is being made and how it may assist in the investigation every time CCTV is reviewed by anyone except as part of routine operations by St George's, University of London security staff. It is split into three sections:

- CCTV viewing by Emergency Services during an Incident. Permission may be granted by St George's, University of London's Incident Controller/Gold Team member or in exceptional circumstances by a security supervisor.
- Review of CCTV by any authorised party that relate to a specific security issue or incident. Permission must be gained from the Director of Estates & Facilities, Facilities Manager and Customer Services Manager.
- Review off CCTV involving images (current or recorded) which will involve the monitoring of staff or students and could lead to action or investigation by Human Resources, Registry, IT or other university departments. Permission must be gained from the Principal.

Requests for information by the police and other authorities must be accompanied by their relevant data protection form signed by the appropriate authority. Disclosure in relation to the prevention or detection of crime and the apprehension or prosecution of offenders may occur without the consent of individual in line with the provisions of data protection legislation.

10. Major incidents

In the event of a major incident, such as public disorder, bomb threat/explosion, serious fire the police will be given the authority to supervise the Security Control Centre. Such authority will be given by Director of Estates & Facilities, Facilities Manager, Incident Controller or Gold Team member verbally or in writing.

11. Signage

Signage has been erected at the main entrances to the university and other locations where CCTV is in use informing that CCTV surveillance is in operation. The sign contains details of the university and a contact number for security.

12. Complaints

Any use of the CCTV systems or material produced which is outside this code and is inconsistent with the objectives of the system will be considered misconduct.

Misuse of the system will not be tolerated. Any person found operating outside this code without good and reasonable course will be dealt with under the university disciplinary procedure.

Complaints received in relation to the use of the CCTV system should be made to the Director of Estates and Facilities or the Facilities Manager.

13. Image Retention

CCTV footage will be retained for a maximum of 31 days, except in cases where a copy has been downloaded in relation to an investigation. These copies may be held for a duration of 12 months.

14. Disposal

At the end of their useful life all discs will have their images erased and disposed of as confidential waste.

15. Review

This code of practice will be reviewed on an annual basis.

May 2018