Policy: CCTV

Department: ITIS

Date: February 2016 **Review Date: 1 year**

1.0 Introduction

This policy describes the acceptable use and management of surveillance systems operated by Goldsmiths. The university uses surveillance systems to protect the university's property and to provide a safe and secure environment for students, staff and visitors.

The processing of personal data occurs where living individuals are identifiable from recordings and the university must ensure that this processing is compliant with the Data Protection Act. This policy is based on the guidance given in the Information Commissioner's Code of Practice. The university takes into account the effect of surveillance systems on individuals and their privacy, with regular reviews to ensure their use remains justified.

2.0 Scope

This policy informs you of what to expect when Goldsmiths College collects personal data via surveillance systems. The term surveillance systems encompasses the following:

- CCTV
- Live surveillance monitors
- Body Worn Video (BWV)

3.0 What information is collected

Our CCTV and live surveillance monitors collect images of individuals who are within their range. Signs are placed at the entrance to the system's zone and within the surveillance area.

BWV collects audio-visual recordings. Staff operating BWV must follow the procedures outlined in the Body Worn Video Procedures.

4.0 Purpose and Assessment

The university as a data controller is required to notify the Information Commissioners' Office to declare the purposes for which it processes personal data. Our Notification states that recordings by surveillance systems may be used for the following purposes:

- To prevent and deter crime
- Assist in the prevention and detection of crime
- Assist with the identification, apprehension and prosecution of criminal offenders
- Monitor the security of campus buildings and property

Before installing surveillance cameras on university premises, the Data Protection Officer will:

- Assess and document the appropriateness and reasons for using the chosen system
- Ensure the reasons are compatible with the declared purposes
- Establish and document who is responsible for ensuring compliance with this policy

5.0 Disclosures

Disclosures of recordings are consistent with the purposes for which they were originally collected as declared in our Notification to the ICO. Judgements about disclosures are made by Goldsmiths College, and we have discretion to refuse any request without an overriding legal obligation, such as a court order or Data Subject Access Request. Disclosures include viewing recording or obtaining a copy of a recording. All viewings take place in a secure, restricted area to ensure that they are confidential.

An internal disclosure is a disclosure made to a member of staff who is not authorised to operate the equipment. In these instances, staff operating the systems are required to keep an internal disclosures log which will be reviewed by the Data Protection Officer.

An external disclosure is a disclosure made to a third party not employed by the university. Third party requesters must complete a third party request form and provide identification at the time of viewing or collection. The disclosure must be approved by the Data Protection Officer or another appointed staff member in her absence. In the case of a disclosure relating to an emergency outside of business hours, please contact the Security Office. These disclosures will only be made in instances where there is a legitimate emergency relating to a natural or man-made disaster or a violent crime. Third parties to whom we may disclose data include:

- Police and other law enforcement agencies where the recordings will assist in a criminal investigation and or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives

It is unlikely that recordings can be disclosed in response to a Freedom of Information request as the requester could potentially use the information for any purposes which would constitute unfair processing under the Data Protection Act.

6.0 Staff Training

The Head of Facilities will ensure that all staff authorised to operate surveillance systems receive training on the operation and administration of the systems.

7.0 Data Subject Access Requests

The Data Protection Act gives individuals the right to access their personal data including recordings made by surveillance systems. Any person wishing to make a Data Subject Access Request in relation to these systems should contact the Data Protection Officer.

A Data Subject Access Request for Lewisham cameras should be sent to:

Crime Reduction Service
CCTV Operations and Development
1A Eros House

Brownhill Road
London SE6 2EF
Tel: 020 8314 6166
Email: control.room@lewisham.gov.uk

A Data Subject Access Request for the Santander campus bank should be sent to:

Data Protection Team
Santander UK plc
Santander House
201 Grafton Gate East
Milton Keynes, MK9 1AN
Tel: 0870 6060 652

8.0 Retention

All recordings are retained for 30 calendar days except when used in conjunction with an investigation or as evidence, in which case they will be retained longer.

8.0 Associated documents

Please refer to:

- Data Protection Policy
- Information Security Policy
- Body Worn Video Procedures
- Notification
- ICO's Code of Practice
- Third Party Disclosures
- List of Goldsmiths CCTV Cameras
- List of Lewisham-controlled CCTV Cameras
- Data Subject Access Request
- ICO "Request your personal information"

9.0 Review of policy

This policy will be reviewed every year or when there are significant changes to it.

10.0 Contact list for queries related to this policy

Data Protection Officer
Chief Information Officer

11.0 Authority for this policy

Senior Management Team