CCTV and Surveillance Technology Policy

Governance and Legal Services
Planning, Strategy and Assurance Directorate
Version 2.0
Approved: March 2016
Review date: March 2018
Key Points

- The university maintains video surveillance technology to deter and assist in the prevention or detection of crime, monitor security and identify actions which might result in disciplinary action.

- The operation of the systems must be consistent with individuals’ rights to privacy.

- Images are likely to be personal data as defined by the Data Protection Act 19998 (DPA) and so must be processed in accordance with the Act, kept secure and destroyed within the agreed retention period. The Information Commissioner’s CCTV Code of Practice must be followed.

- Individuals have rights to access images of themselves.

- Thirds parties may request copies of images in specified circumstances. This likely to be to law enforcement agencies, prosecution agencies and appropriate members of university staff.

- Signs must be prominently displayed informing people that monitoring is in use.

- Covert monitoring must only be carried out with the authorisation of the Senior Vice-President (Operations) (or a nominee).

- The Estates and Facilities Compliance Manager is responsible for compliance with and implementation of this policy.

- The Head of Information Management and Compliance is responsible for advising on compliance with the DPA and other legislation in relation to surveillance technology.

- The Director of Governance and Legal Services is accountable for ensuring compliance with the policy.

1. Purpose

1.1 This policy sets out the accepted use and management of video surveillance systems or any other surveillance technology including CCTV to ensure the university complies with its legal obligations and respect for individual privacy of its students, staff, contractors and visitors.

2. Scope and definitions.

2.1 This policy covers the use of surveillance technologies which record identifiable images of people on university premises.

2.2 CCTV is defined as: fixed cameras designed to capture and record images of individuals.

2.3 Surveillance System is defined as: any electronic system or device that captures images of individuals or information relating to individuals. This term is used in this policy to refer to any surveillance technology including CCTV. It includes any technology that may be introduced in the future for a similar purpose such as automatic number plate recognition (ANPR), body worn cameras or aerial surveillance.

2.4 Current Video Surveillance systems

2.4.1 The university has in place video surveillance systems to provide a safe and secure environment for students, staff and visitors, and to protect university property.
2.4.2 The university carries out Threat and Security Risk Assessments as required by British and European standards to identify where there is a requirement for video surveillance technology. Reasons for a decision to install may include but are not limited to the following:

- Deter crime
- Assist in prevention and detection of crime
- Assist with the identification, apprehension and prosecution of offenders
- Assist with the identification of actions that might result in disciplinary proceedings against staff and students
- Monitor security of campus buildings
- Identify vehicle movement problems around the campuses

2.5 Operation of the systems

- The systems will be provided and operated in a way that is consistent with an individual’s right to privacy.
- Video surveillance systems operate continually.
- Responsibility for management of the systems is with the Estates and Facilities Directorate.
- Surveillance cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. All cameras will be positioned to only capture images from the areas intended as detailed in site specific Security Risk Assessments (SRA).
- 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. These must state that monitoring is in use, the name of the organisation responsible, the reason for the monitoring and give contact details for any enquiries.

2.6. The systems will not be used to:

- Provide images to the world wide web
- Record sound
- Disclose to the media

3. Legislative framework

3.1 Relevant legislation is:

- The Data Protection Act 1998 (DPA). This covers the rights of individuals (data subjects) in respect of their personal data. Identifiable images of individuals are personal data.
- The Human Rights Act 1998 (HRA) enshrines “respect for private and family life.”

3.2 For the purpose of the DPA King’s College London is the data controller.
3.3 The university has produced this policy in line with the Information Commissioner’s (ICO) CCTV Code of Practice 2015.

3.4 Digital images

If images show a recognisable person, they are personal data and are covered by the Data Protection Act 1998. The university’s Data Protection Policy, should be adhered to at all times. It is overseen by the Information Management and Compliance Team.

3.5 The university is required to register its processing of personal data (including images) with the Information Commissioner’s Office (ICO). The university’s ICO notification registration number is Z7915194, renewed annually in December.

3.6 Where new cameras are to be installed on university premises, the ICO’s CCTV Code of Practice will be followed before installation including the following:

- The appropriateness of and reasons for using video surveillance will be assessed and documented;
- The purpose of the proposed surveillance system will be established and documented;
- Responsibility for day-to-day compliance with this policy will be established and documented;
- Consultation with the Information Management and Compliance team is required to ensure that the video surveillance system is covered by the university’s Notification with the Information Commissioner’s Office (ICO);
- Where new uses are proposed for video surveillance systems, these should be subject to a Privacy Impact Assessment (PIA) in accordance with the ICO Code of Practice on Privacy Impact Assessment.

3.7 Individual access rights

3.7.1 The Data Protection Act 1998 gives individuals the right to access personal information about themselves, including images.

3.7.2 All requests for access to a copy of video footage by individuals should be made in writing to the Information Management and Compliance Team (IMC). The university’s Subject Access Request form may be used. IMC will liaise with relevant security staff in the Estates and Facilities Directorate to determine whether disclosure of the image will reveal third party information.

3.7.3 Requests for access to CCTV images must include:

- The date and time the images were recorded
- Information to identify the individual, if necessary
- Proof of identity
- The location of the camera

3.7.4 The university will respond promptly and at the latest within 40 calendar days of receiving the £10 request processing fee and sufficient information to identify the images requested.

3.7.5 If the university cannot comply with the request, the reasons will be documented.

3.7.6 The requester will be advised of these in writing, where possible.
3.8 Access to images by third parties

3.8.1 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 necessarily 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.

3.8.2 Routine access to images will be restricted to those staff that need to have access in accordance with the purposes of the system.

3.8.3 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following:-

- Law enforcement agencies (where the images recorded would assist in a specific criminal enquiry, and at the university’s discretion).
- Prosecution agencies.
- Appropriate members of university staff (such as Human Resources and the Student Conduct, Complaints and Appeals team) in the course of staff or student disciplinary proceedings (including prospective proceedings) to ensure compliance with the university’s regulations and policies.
- The King’s College London Students’ Union (KCLSU), in accordance with the university’s data sharing agreement with the KCLSU, where necessary for maintaining a safe environment in the premises occupied by the KCLSU or for ensuring compliance with either party’s regulations or policies (including use in disciplinary proceedings).
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries).
- King’s Health Partners (KHP), where incidents occur on shared or adjacent premises. This must be covered by a suitable non-disclosure agreement or Data Sharing agreement which limits access to the images to staff of the relevant KHP organisation with a legitimate reason to see it.

3.8.4 All third party requests for access to a copy of video footage should be made in writing to the Information Management and Compliance team. If a law enforcement or prosecution agency is requesting access they should make a request under Section 29 of the Data Protection Act 1998.

3.8.5 Images that have been recorded may be viewed on site by the individual whose image has been captured and/or a uniformed police officer when responding to routine incidents which occurred on the same day. No copies may be taken off site. Please use the form at Appendix A to record the details of these requests.

3.9 Requests to prevent processing

3.9.1 In addition to rights of access, Data Subjects also have rights under the DPA to prevent processing (i.e. monitoring and recording CCTV images) likely to cause substantial and unwarranted damage to that person, or prevent automated decision taking (i.e. through the use of visual recognition software) in relation to that person.

3.9.2 Should a Data Subject have any concerns regarding the operation of the CCTV systems, the
following procedure must be complied with:

- The Data Subject should be directed to the Information Management and Compliance team to determine whether the Data Subject is making a request to prevent processing or automated decision making. If the Information Management and Compliance team determines that the Data Subject is instead making a Subject Access Request, the procedure will be followed.

- The Information Management and Compliance Team will consider the request to prevent processing or automated decision making in consultation with appropriate staff in the Estates and Facilities Directorate.

3.9.3 The Information Management and Compliance team will normally provide a written response within twenty-one days of receiving the request to prevent processing or automated decision making, setting out their decision on the request. A copy of the request and response will be retained. Any other person with complaints or queries regarding the video surveillance system and its operation must be made in writing to Estates and Facilities Compliance Support Manager

3.10 Retention and disposal

3.10.1 Unless required for evidential purposes or the investigation of crime or otherwise required by law, recorded images will be retained for no longer than 90 days from the date of recording.

3.10.2 At the end of their useful life all images stored in whatever format will be erased securely and permanently and where in physical form for example tapes or discs, disposed of as confidential waste. All still photographs and hard copy prints also will be securely disposed of as confidential waste.

3.11 Covert monitoring

3.11.1 Covert monitoring (where the individual is not aware the monitoring is taking place) will only be justifiable in exceptional circumstances where there are grounds to suspect criminal activity or extremely serious malpractice. If such monitoring is undertaken:

- It must be with the authorisation of the Senior Vice-President (Operations) (or a nominee);
- The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom;
- It 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 risk of intrusion on innocent workers is considered;
- Areas where a high level of privacy is expected remain private;
- Only limited numbers of people will be involved in the monitoring.

3.12 Access to images by staff

3.12.1 Access will be restricted to those staff that need to have access in accordance with the purposes of the system.
4. Accountability and Responsibility

4.1 The CCTV surveillance system is owned by King’s College London.

4.2 Data Governance and Strategy Group are responsible for approving and reviewing this policy.

4.3 The Policy Lead is: Head of Information Management and Compliance

4.4 The Estates and Facilities Compliance Manager is responsible ensuring compliance with this policy.

4.5 Authorisation for new CCTV camera installations or other installation or use of surveillance technologies must be given in writing by the Estates and Facilities Compliance Manager.

4.6 The Director of Governance and Legal Services is accountable for ensuring compliance with the policy.

4.7 The Head of Information Management and Compliance is responsible for advising on compliance with the DPA and other legislation.

5. Monitoring

5.1 This Policy will be reviewed not less than every two years or when the law or guidance changes.

Head of Information Management and Compliance
James Clerk Maxwell Building
57 Waterloo Road
London
SE1 8WA
Tel: 0207 848 1380
Email: info-compliance@kcl.ac.uk

5.2 The Information Management and Compliance team is responsible for:

- Maintaining this policy
- Providing expert guidance on the application of the DPA
- Providing guidance regarding subject access requests and third party requests for access to footage.
- Providing guidance, support and training
- Liaison with the Information Commissioner’s Office, including annual notification to the ICO

6. Associated policies and guidance

- Data Protection Policy
- Data Protection – Sharing Personal Data
- In the picture: a data protection code of practice for surveillance cameras and personal information. ICO, 2015
- Information Security Policy
King’s College London
Routine request for access to CCTV images

This form should be used for routine requests for access to view CCTV images by individuals whose images have been captured and/or uniformed police in response to incidents which occurred on the same day e.g. to assist in a specific criminal enquiry, identify a victim, witness or perpetrator in relation to a criminal incident.

This form should **not** be used where the police or other law enforcement agencies request a *copy* of CCTV images. A Section 29 request should be made under the Data Protection Act 1998 for this type of access. Please refer to the Information Management and Compliance team.

This form should **not** be used an individual whose image has been recorded requests a *copy* of CCTV images relating to themselves. A subject access request under the Data Protection Act 1998 is required for this type of access. Please refer to the Information Management and Compliance team.

<table>
<thead>
<tr>
<th>To be completed by Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
</tr>
<tr>
<td>Person making request</td>
</tr>
<tr>
<td>Organisation</td>
</tr>
<tr>
<td>Reason for request</td>
</tr>
<tr>
<td>Crime reference number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To be completed by KCL representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason for allowing access/disclosure</td>
</tr>
<tr>
<td>Reason for refusing access/disclosure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name &amp; Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Position</td>
</tr>
<tr>
<td>Date</td>
</tr>
</tbody>
</table>