PROCEDURE:	**CCTV, Surveillance and Access Control Systems**
Related Procedures:	Requests for Personal Information Procedure Data Breach Management Procedure
Related College Policies:	Policy on CCTV, Surveillance and Access Control Systems Information Security Policy Data Protection Policy
Effective Date:	5 December 2019
Supersedes:	March 2016
Next Review:	31 July 2023

---

1. Purpose & Scope

1.1 This procedure is intended to support the policy on CCTV, Surveillance and Access Control Systems. The procedure provides a framework for the operation of those systems and for the use of the data which is recorded and stored by them.

1.2 The procedure provides a framework for ensuring that the use and management of such security technology by the university complies with its legal obligations to respect individual privacy rights.

1.3 This procedure covers the use of surveillance technologies including CCTV and access control systems which record personal data relating to individuals on university premises, where the university is the controller of the data. The procedure also covers technology which monitors space to support more efficient building management, space and energy use. It has been designed to ensure that the practices adopted by the university are consistent with the Information Commissioner's (ICO) CCTV Code of Practice 2017.

2. Definitions

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

2.2 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.

2.3 Systems data is defined as any personal data held or captured by a video surveillance or access control system.

2.4 Building monitoring technology is defined as equipment which provides aggregated and anonymised data on the occupation of university space.

2.5 Security Systems Technicians are employees of the university, working within the Estates & Facilities Directorate, to maintain the door and controller hardware associated with the access control system.

2.6 Staff is defined as those individuals employed directly by the university.

2.7 Contractors are defined as employees of companies contracted to supply a service to the university.

3. Procedure

3.1 Summary Points

3.1.1 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.

3.1.2 The lawful basis for processing data is Legitimate Interests. The operation of the systems must be consistent with individuals' rights to privacy, and other rights under the General Data Protection Regulations (GDPR).

3.1.3 Images are likely to be personal data as defined in the prevailing Data Protection legislation must be processed in accordance with law, kept secure and destroyed within the agreed retention period.

3.1.4 Third parties may request copies of images and recorded data in specified circumstances. This is likely to be to law enforcement agencies or prosecution agencies. Images and data may be provided to university staff for the purposes of operational management or for a legitimate investigation under university procedures. In all cases, information will only be provided following appropriate approval.

3.2 Video Surveillance

3.2.1 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.

3.2.2 The university will decide where to install video surveillance technology based on a Threat and Security Risk Assessment (SRA) conforming to British and European standards. Cameras will only be installed after an SRA has been carried out.

3.2.3 In line with these standards, reasons for install surveillance equipment may include but are not limited to the following:

- To deter crime
- To assist in the prevention and detection of crime or the identification, apprehension and prosecution of offenders
- To assist with the identification of actions that might result in disciplinary proceedings against staff and students
- To monitor security of campus buildings
- To manage events
- To identify vehicle movement problems around the campuses

3.2.4 Surveillance cameras are located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. Cameras will be positioned only to capture images from the areas identified in the site-specific SRA.

3.2.5 Where new cameras are to be installed on university premises, the ICO's CCTV Code of Practice will be followed before installation is made. The steps taken are as follows:

a) Assess and document the appropriateness of, and reasons for, using the proposed video surveillance;

b) Establish and document the purpose of the proposed surveillance system;

c) Establish and document how day-to-day compliance with the university CCTV policy will be maintained for proposed installation;

d) Consult the Information Compliance team to ensure that the proposed video surveillance system is covered by the university's Record of Processing Activities

e) If new uses are proposed for video surveillance systems which may result in a risk to the rights and freedoms of individuals, undertake a Data Protection Impact Assessment (DPIA or PIA) in accordance with the ICO Code of Practice on

Privacy Impact Assessment;

f) If new technologies, e.g. ANPR, are considered as part of the university's video surveillance estate, a DPIA or PIA should also be carried out in accordance with ICO guidance.

3.2.6 Signs will be prominently displayed 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 and any other details required by prevailing law or ICO guidance.

3.2.7 The CCTV or video surveillance systems will not be used to:

- Provide images to the world wide web
- Record sound
- Disclose to the media unless in co-operation with public appeal in a police investigation

3.3 Individual access rights to data recorded by the systems

3.3.1 Anyone who believes they have been filmed by the system can request a copy of the recording, subject to the restrictions of the relevant data protection legislation.

3.3.2 Requests should be made using the Subject Access Request process of the university and should include all information necessary to locate the image on the recording system. Data subjects can also exercise their other Data Subject Rights through this same process.

3.3.3 Requests must include the following information:

- The date and time the images were recorded;
- Detailed information to identify the individual;
- Proof of identity; and
- The precise location of the camera.

3.3.4 Data subjects also have the right to request that inaccurate data be corrected or erased and to seek redress for any damage caused. This right can be exercised by contacting the Information Compliance team, using the Subject Access Request process of the university.

3.3.5 Where the university is unable to comply with the request, the requester will be notified in writing.

3.3.6 Individuals have the right to request information relating to their access to areas of the campus which are recorded on the Access Control System. In this instance, requests should be made using the Subject Access Request process of the university and should contain all information necessary to identify the required data, including the name of the data subject, their King's Identity Number and relevant dates.

3.3.7 Data subjects can also exercise their other Data Subject Rights through this same process.

3.4 Access by third parties to data recorded in the systems

3.4.1 Unlike Data Subjects, third parties do not have a right of access information held on the security systems except in exceptional circumstances. They do not necessarily have a right of access under the GDPR, and care must be taken when complying with such requests to ensure that neither the GDPR nor the CCTV, Surveillance and Access Technology Policy is breached.

3.4.2 Access to information will be restricted to those staff or other individuals or agencies that need to have access in accordance with the purposes of the system, to undertake their legitimate duties or to discharge their responsibility towards the university.

3.4.3 Disclosure of video recordings or data held on security systems will only be made to third parties in strict accordance with the purposes of the system and the prevailing data protection legislation. It is limited to the following:

- 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 investigations and to provide an evidential basis for proceedings brought under other regulations and policies of the university;
- Law enforcement agencies, where the images recorded would assist in a specific criminal enquiry, and at the university's discretion;
- Other agencies with statutory powers to investigate or prosecute;
- The King's College London Students' Union (KCLSU), in accordance with the university's data sharing agreement with the KCLSU and where the information is necessary for maintaining a safe environment in the premises occupied by the KCLSU or for ensuring compliance with the regulations or policies of either party; or
- The hospital Trusts which make up the King's Health Partnership (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 Trust organisations with a legitimate reason to see it.

3.4.4 All third-party requests for access to a copy of video recordings or data held on security systems should be made in writing to the Information Compliance team. If a law enforcement or prosecution agency is requesting access, they should make a request under the relevant Data Protection legislation.

3.4.5 In certain emergency situations university staff may have to make quick decisions about sharing data, such as when there is a danger to the health of a person. Neither data protection legislation nor the Policy on CCTV, Surveillance and Access Technology prevent staff from data sharing in urgent situations so long as the sharing is necessary and proportionate to the situation.

3.4.6 The ICO's data sharing code of practice says the following on data sharing in moments of urgency or emergency:

> "Sometimes you may have to make a decision quickly about data sharing in conditions of real urgency, or even in an emergency situation. You should not be put off from data sharing in a scenario like this; in an urgent situation you should do what is necessary and proportionate."

In an emergency situation:

- The emphasis should be on doing what is necessary and proportionate in the circumstances.
- You should factor in the risks involved in not sharing data in emergency situations. Data protection legislation does not prevent the sharing of data in situations where there is a danger to the health of a person.

3.4.7 The authorisation route for releasing CCTV data to third parties is shown in Appendix A.

3.4.8 The authorisation route for releasing data from the access management systems to third parties is shown in Appendix B.

3.4.9 The reason for release of information to a third party must be fully documented as part of the procedure. The form attached to this Procedure at Appendix C must be used to apply for the release of data so that the reasons for request and approval/refusal are fully documented and tracked for audit.

3.4.10 Images that have been recorded may have to be viewed on site by the individual whose image has been captured and/or a uniformed police officer when responding to incidents which occurred on the same day. In this instance, no copies may be taken off site without going through the approval process described above.

3.4.11 Where an image is viewed on the same day as an incident, the authorisation form at Appendix C should be completed for an audit trail.

3.5 Requests to prevent processing of CCTV images

3.5.1 In addition to rights of access, Data Subjects also have rights under the relevant data protection legislation to restrict processing (i.e. monitoring and recording surveillance images) and have the right to erasure (the right to be forgotten). Should a Data Subject have any concerns regarding the operation of the surveillance systems, the following procedure must be complied with:

- The Data Subject should be directed to the Information Compliance team to determine which right the Data Subject is making a request in regard to.
  - If the Information Compliance team determine that the Data Subject is instead making a Subject Access Request, that procedure will be followed.
- The Information Compliance Team will log the request to prevent processing or automated decision making and consider it in consultation with appropriate staff in the Estates and Facilities Directorate.

3.5.2 The Information 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 the university's decision on the request.

3.6 Access Control system data

3.6.1 The data held by the university in relation to the Access Control System includes:

- Cardholder data
  - First name
  - Middle name
  - Last name
  - Title
  - Department
  - Course code
  - Course short name
  - Email address
  - Student/employee code
  - Student/staff number (K number)
  - Mobile number
- Cards allocated to cardholders
- Locations, dates and times of card reads

3.6.2 The access control data is accessible by staff who require the access control terminal software to carry out their duties. This includes:

- Security Technicians
- Security staff who issue cards and alter access rights

- Managers of the Security staff mentioned above
- Library employees
- Student Services
- The Assurance Manager (Security)
- The Assurance Support Manager – (Security)
- IT application support employees
- *Welcome to King's* enrolment team members
- Residences reception employees
- The St Thomas' Campus Technical Manager

3.6.3 Where data is released from the access control system, in compliance with the processes set out in this Procedure, where practically possible, all fields which make the data identifiable as belonging to a specific person should be removed. For example, if a request to know how many people used a reader during a certain period, the report need not include the names of the cardholders, their photographs, or any other personal information, just the quantity of card reads.

3.7 Retention and disposal

3.7.1 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 the recording.

3.7.2 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, discs, disposed of as confidential waste. All still photographs, and hard copy prints also will be securely disposed of as confidential waste.

3.7.3 All information and data storage and retention must conform to the university Retention Schedule.

3.8 Legislative framework

3.8.1 The applicable legislation is:

- The Data Protection Act (2018) and then the General Data Protection Regulation and any other applicable privacy laws. This covers the rights of individuals as data subjects in respect of their personal data.
- The Human Rights Act 1998 (HRA) enshrines "respect for private and family life."

3.8.2 For the purpose of applicable Data protection laws, King's College London is the data controller.

3.9 Accountability and responsibility

3.9.1 The CCTV surveillance system and the door access system are owned by King's College London.

3.9.2 The Director of Operations is accountable for ensuring compliance with the policy.

3.9.3 The Policy Lead is the Associate Director of Assurance and Business Risk, and they are responsible for ensuring the Policy and Procedure are reviewed The Operational Assurance and Risk team in Estates and Facilities act on behalf of the Director of Operations for delivery and governance.

3.9.4 The Estates and Facilities Assurance Manager (Security) acts for and on behalf of the Policy Lead and is responsible for reviewing the Policy and Procedure and ensuring compliance with both.

3.9.5 The Operational Assurance team is responsible for the authorisation of new CCTV camera installations or door access controls. The authorisation process will be facilitated by the Assurance Manager (Security).

3.9.6 The Information Compliance team is responsible for advising on compliance with the Data Protection legislation and managing Subject Access Requests under the CCTV, Surveillance and Access Technology policy and procedure.

3.10 Complaints procedure

3.10.1 Any other person with complaints or queries regarding the video surveillance system or the door access control system and their operation must be made in writing to the Estates and Facilities Operational Assurance and Risk Team assurance-estates@kcl.ac.uk.

3.11 Monitoring

3.11.1 This procedure will be reviewed every three years, alongside the policy, or when the law or guidance changes.

3.11.2 For more information about CCTV, surveillance or access control systems contact:

Associate Director of Assurance and Business Risk
3rd floor
5-11 Lavington Street
London
SE1 0NZ

Tel: 0207 848 3456
Email: ask@kcl.ac.uk

4. Associated policies and guidance

King's College London Data Protection Policy

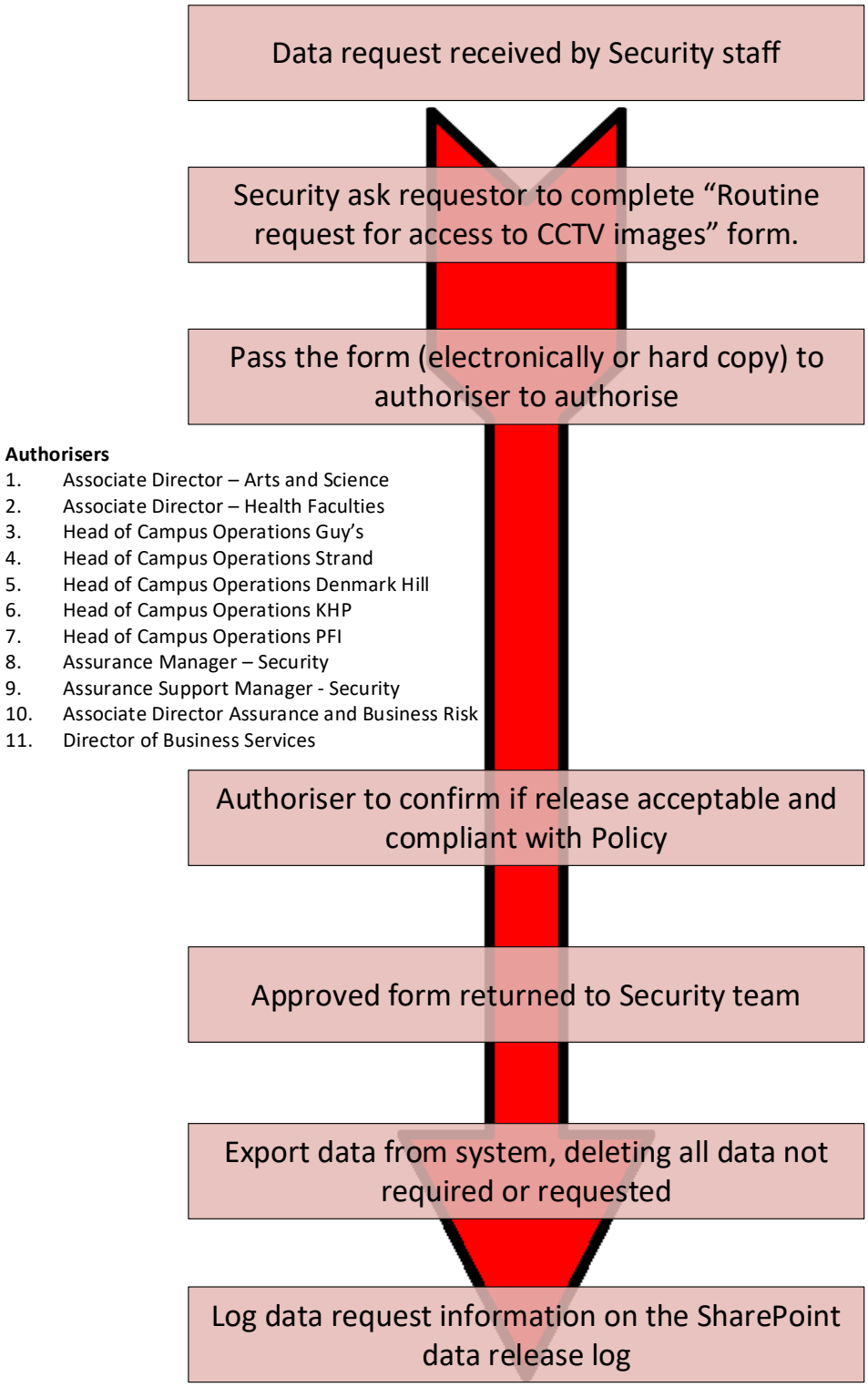
In the picture: a data protection code of practice for surveillance cameras and personal information. ICO, 2017

King's College London Information Security Policy

Data Protection – Sharing Personal Data

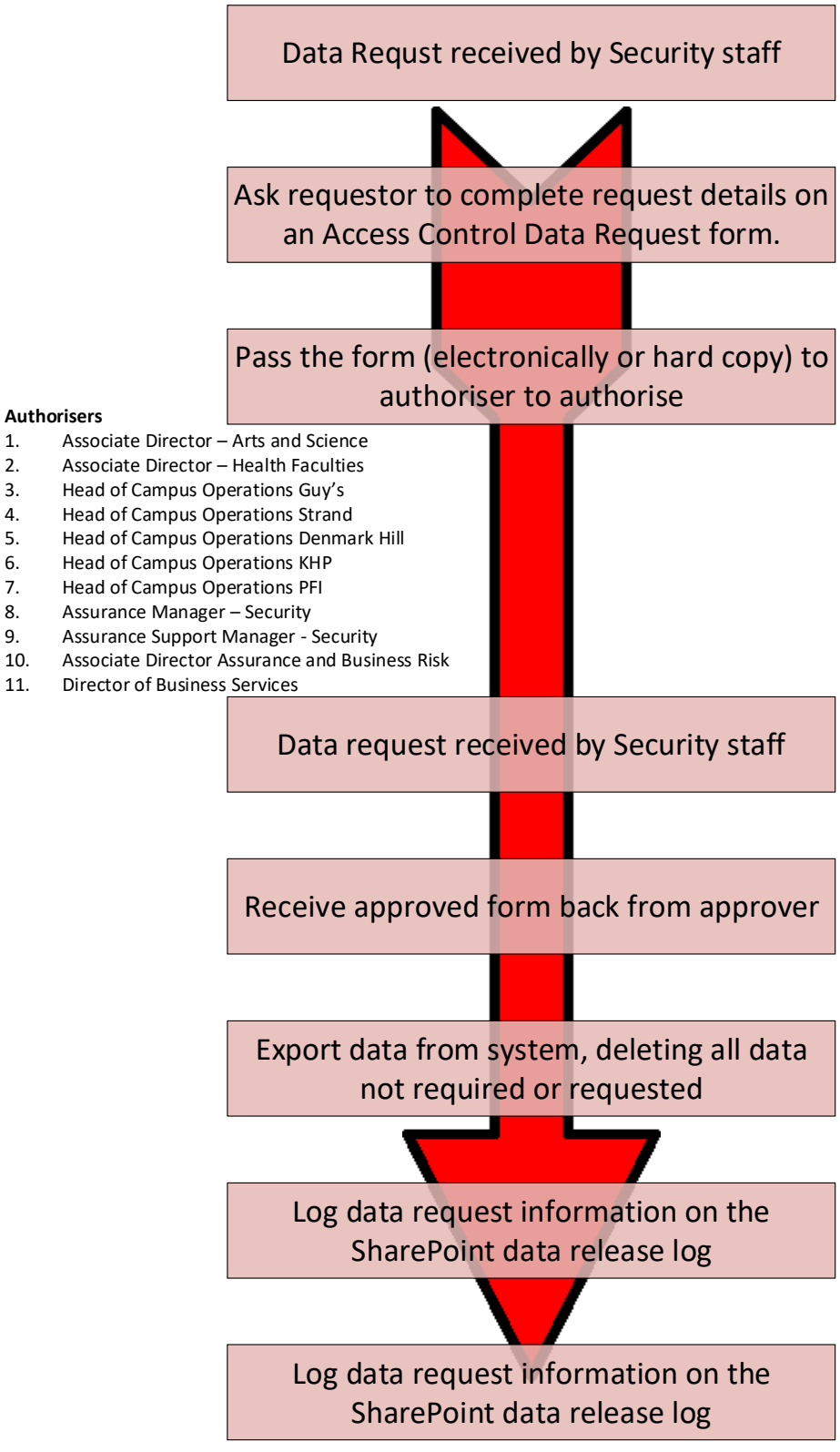
Appendix A

THIRD PARTY CCTV DATA REQUEST PROCESS



Appendix B

ACCESS CONTROL DATA REQUEST PROCESS



Appendix C

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. These requests should be made under the relevant Data Protection legislation for this type of access. Please refer to the Information Compliance team.

This form should **not** be used where an individual whose image has been recorded requests a *copy* of CCTV images relating to themselves. A subject access request under the relevant data protection legislation is required for this type of access. Please refer to the Information Compliance team.

To be completed by Applicant

Date	
Person making request	
Organisation	
Reason for request	
Crime reference number	

To be completed by KCL representative

Reason for allowing access/disclosure	
Reason for refusing access/disclosure	
Name & Signature	
Position	
Date	