Imperial College London

CCTV Code of Practice

Incorporating Automatic Number Plate Recognition systems

Edition: May 2018

CONTENTS:

1. Introduction and Accountability

Following the Government's commitment to further regulate Closed Circuit Television (CCTV), the Protection of Freedoms Act 2012 (PFA) provided for the development of a Code of Practice relating to CCTV, Automatic Number Plate Recognition (ANPR) and other surveillance camera systems, and the appointment of a Surveillance Camera Commissioner.

The 'Surveillance Code of Practice' pursuant to the Protection of Freedoms Act 2012 was published in August 2013. It will help ensure that a system operator makes transparent decisions about the legitimacy and proportionality of surveillance.

This Code of Practice covers the College's CCTV and ANPR systems and is intended to reflect the spirit and guidance issued by the Information Commissioner's Office, as documented in the 'Protection of Freedoms Act 2012'.

Closed Circuit Television

a) Imperial College London ('The College') is the owner of public closed circuit television (CCTV) systems currently installed on its campuses and in/on College property off campus. The Head of the Security Department at the College retains overall responsibility for the system and delegates the day to day management to the Deputy Head of Security

b) All images produced by the system remain the property of the College.

c) The vast majority of our cameras are overt, with the images recorded centrally, and are all viewable centrally by trained Security staff. In addition, a limited number of management staff have the facility to monitor cameras sited within their own areas of responsibility. The cameras cover roadways, car parks, buildings, vulnerable public facing offices and some licensed premises. See also 'Covert filming or monitoring' section, below.

d) The primary Security Control room is situated on the ground floor of the Sherfield Building South Kensington Campus, London, SW7 2BX, and is staffed 24 hours a day, 365 days per year by trained, uniformed Security Officers; there is also an alternate control room on the South Kensington site and one at Silwood Park campus Buckhurst Road, Ascot, Berks, SL5 7PY.

e) The primary and Silwood park Control Rooms also have Home Office licensed radio systems installed, linking the Control Rooms with trained Security Officers who provide mobile and foot patrols of the campuses and are able to respond to incidents identified on the CCTV monitors.

f) Unlawful access to the data and images is prevented by swipe control ID and key access to secure areas, 24 hour manning, and controlled IT system login.

Automatic Number Plate Recognition System

a) Parking at the College's South Kensington and Silwood Park Campuses is operated and controlled using an Automatic Number Plate Recognition system (ANPR). The Director of Estate Facilities at Imperial College London retains overall responsibility for the system, and has delegated the day to day management of the system to the Security Team.

b) Cameras are located at the entrances and exits to campuses, where images of vehicle number plates are captured and remain the property of the College.

c) The ANPR system provider for South Kensington is Sagoss, through which their server hosts both the cameras and the payment kiosks linked to the system. At Silwood the ANPR system is provided by PIPS Technology. The College reserves the right to vary its systems providers whilst ensuring the principles within this code are met.

d) All images for South Kensington are viewable centrally by approved and trained members of its Security Services Team located on the Ground Floor of the Sherfield Building and staffed Monday – Friday from 7am – 4pm. Those at Silwood are viewed locally by approved and trained Security staff.

2. Objectives

Objectives of the CCTV Schemes:

To assist in providing a safe and secure environment for the benefit of those who might visit, work or live within the College's campuses. Subject to this Code of Practice the schemes will not be used to invade the privacy of any individual residence, business or other private premises, buildings or land, and are for the purposes of parking control and enforcement and the good and safe management of its car parks, furthering compliance with the College's Parking Regulations.

The CCTV systems will only be used for the following purposes and within this Code of Practice.

- To reduce the fear of crime and to reassure students, staff and visitors.
- To deter and detect crime, public disorder and anti-social behaviour.
- To identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour.
- To provide the College with evidence upon which to take criminal and civil action.
- Staff and student discipline: The College will only use the images in a staff disciplinary case when there is suspicion of misconduct and not to generally monitor staff activity; likewise the images will only be used as evidence in serious student disciplinary cases being heard by the College Discipline Committee and the Head of Security Services or other higher authority.
- To monitor and assist with parking and traffic management issues.
- To assist in the monitoring and deployment of staff during emergency situations.
- Upon formal request, to assist Police and other law enforcement agencies with the pursuit of their objectives.

Covert filming or monitoring:

Covert filming or monitoring may be used as part of a specific time-limited investigation where informing subjects of, or signposting the activity would have a prejudicial effect on that investigation. The decision to use covert monitoring as a proactive investigation tactic may only be taken after consultation with the Head of Imperial College Security or Security Operations Manager in his/her absence and with written authorisation from the College Secretariat. Covert monitoring shall only be used for the prevention and detection of criminal activity or equivalent malpractice.

Objectives of the APNR Schemes:

Automatic Number Plate Recognition is used by the College for the purposes of parking control and enforcement and the good and safe management of its car parks, furthering compliance with the College's Parking Regulations. On occasion, College Managers, in the course of investigating incidents or accidents, or undertaking Staff or Student disciplinary proceedings may need controlled access to ANPR data.

The ANPR systems will only be used for the following purposes and within this Code of Practice.

- To ensure that arrangements for the limited car parking spaces available across our London campuses are more consistent.
- To assist with reducing congestion in and around the campus.
- To prevent unauthorised use of the car parks.
- To assist with investigations in conjunction with The Security Department.
- To assist with the provision of a smoother, more efficient parking experience for members of the public.

3. A). Data Protection

a) The College is committed to complying with the requirements of the General Data Protection Regulation (GDPR) and intends to operate the system in accordance with the data protection principles set out in the GDPR.

b) The standards, which must be met if the requirements of the GDPR are to be satisfied, are based on the data protection principles set out in Article 5 of the GDPR which are:

1. personal data shall be processed lawfully, fairly and in a transparent manner;

2. personal data shall be collected for specified, explicit and legitimate purposes only, and will not be processed it in a way that is incompatible with those legitimate purposes;

3. only personal data that is adequate, relevant and necessary for the relevant purposes shall be processed;

4. personal data must be accurate and must be kept up to date; reasonable steps must be taken to ensure that inaccurate personal data are deleted or corrected without delay;

5. personal data can be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed; and

6. appropriate technical and organisational measures must be taken to ensure that personal data are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

   The College (as controller in most cases where it processes personal data) is also responsible to demonstrate compliance with the above data protection principles.

All members of staff involved in operating the system will be made aware of the objectives of the scheme and will be permitted only to use the system to achieve those objectives.

The College's Data Protection Policy is available on this link.

3 B). CCTV/ANPR Guiding Principles

The College has adopted the following 12 guiding principles of the Code:

"1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date."

The College recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of staff should be aware of the restrictions relating to this set out in this Code and the rights of individuals under the GDPR and the Surveillance Camera Code of Practice (SCCoP).

4. Administration

CCTV:

a) It is the responsibility of the Head of the Security Department (or Deputy in his/her absence) to:

- Select camera sites and initial areas to be viewed.
- Be responsible for compliance with the GDPR and SCCoP.
- Take responsibility for control of the images and make decisions on how these can be used.
- Ensure the system is secure and only viewed by authorised personnel.
- Ensure that the procedures of this Code of Practice comply with the current data protection law and SCCoP.
- Introduce a CCTV incident log and record of Police or other Statutory Authority requests for images.
- Bi-annual checks by the Head of the Security Department or Deputy Head of Security to establish that nominated area managers still require viewing rights of the system in line with the above objectives
- Ensure adequate signage is erected.
- Regularly evaluate the system and its usage to ensure it continues to comply with the latest legislation, CCTV Codes of Practice.

b) It is the responsibility of the Head of the Security Department to:

- Clearly communicate the specific purposes of the recording of and use of images and objectives to all Security staff.
- Ensure that a CCTV incident log and record of Police or other Statutory Authority requests for images is maintained.
- Carry out audit checks at 6 monthly intervals (at a minimum) to check that procedures are being correctly followed. Records of audits to be kept.

c) It is the responsibility of the individual operating officers to:

- Select appropriate images to be recorded on controllable cameras (Pan-Tilt-Zoom (PTZ)) so as to comply with the objectives outlined above.
- Ensure that targeting of individuals with the cameras is only conducted when there is reasonable suspicion that the person falls within one of the objectives set above e.g. committing a criminal offence or engaging in anti-social behaviour.
- Not to view into private property and be mindful of privacy within College owned accommodation.
- Complete the Imperial College Crime Report and obtain the data release form as appropriate.

ANPR:

It is the responsibility of the Head of Security or deputy in his/her absence to:-

- Ensure that all ANPR equipment is working correctly.
- Be responsible for compliance with the GDPR and SCCoP.
- Take responsibility for control of the images and make decisions on how these can be used.
- Ensure the system is secure, and only viewed by authorised personnel.
- Ensure that the procedures of this Code of Practice comply with the GDPR and SCCoP.
- Introduce an ANPR incident log and record of Police or other Statutory Authority requests for images.
- Bi-annual checks by the System Manager to establish that authorised operators require viewing rights of the system in line with the above objectives

- Regularly evaluate the system to ensure it continues to comply with the latest legislation.

It is the responsibility of the Head of Security or deputy to:

- Clearly communicate the specific purposes of the recording of and use of images and objectives to all authorised operators
- Ensure that an ANPR incident log and record of Police or other Statutory Authority requests for images is maintained
- Carry out annual audits to check that procedures are being complied with
- Ensure that the audit team include ANPR practices and procedures on their regular audits of the Estates Facilities Department

5. Storing and Viewing Images

a) All images recorded on the College's CCTV cameras are digitally stored on computer/server hard drives, and although the images can be searched, it is not possible to tamper or alter them. The ANPR images are stored on the system and can be searched but not altered.

b) In the event of the Police requiring CCTV images they can be 'burnt' onto a CD/DVD for evidence in court, on receipt of the appropriate Data Protection form. ANPR images can also be printed, also upon the receipt of appropriate Data Protection forms.

c) The CCTV images over record after 30 days, however any relevant images can be locked on the hard drive for future reference. ANPR images are kept for 6 months and then purged from the system unless required for operational needs. All retained images are subject to the controls outlined in these procedures.

d) Viewing of live images on monitors is restricted to Security/ANPR operators and other authorised personnel and can only be accessed using passwords.

e) Images are viewed in confidence in secure private offices.

f) Requests to view images or image disclosure of third parties should be made in writing to the Head of the Security Department.

6. Disclosure of images to third parties

a) The following guidelines will be adhered to in relation to disclosure of images:
   - Will be in line with the objectives (see 3B above)
   - Will be controlled under the supervision of the Head of the Security Department or his/her Security Managers
   - A log book/sheet will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for disclosure
   - The appropriate disclosure documentation from the Police will be attached to the log entry
   - Images **must not** be forwarded to the media or be placed on the internet or otherwise distributed without specific and written prior approval of the College Central Secretariat acting in compliance with the law and these procedures. Failure to comply will result in disciplinary action being taken. Images will only be released to the media for legitimate purposes (e.g. identification of data subjects) and in liaison with the Police or other law enforcement agency.

b) Any other requests for images should be routed via the Head of the Security Department, as disclosure of these may be unfair or unlawful to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of individuals whose images are recorded.

c) The College has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body such as the Police, then they become the data controller for their copy of that image. It is their responsibility to comply with the GDPR in relation to any further disclosures.

7. Signage

Signage has been erected at the main entrances to the College campuses and at other locations where CCTV is in use, stating that CCTV and ANPR systems are in operation.

It is the responsibility of the Head of the Security Department to ensure that adequate signage is erected to comply with the Information Commissioner's Code of Practice.

8. Disclosure of images to the data subject (Subject Access Requests)

Individuals whose images are recorded have a right to view the images of themselves, or their vehicles and, unless they agree otherwise, to be provided with a copy of the images. All such requests are handled by the College's Data Protection Officer in liaison with the Head of the Security Department (for CCTV) or the Estate Facilities Campus Coordinator (for ANPR).

- Images must be provided within 40 calendar days of the request being received.
- Those who request access must provide proof of identity and details which allow the College to identify them as the subject of the images and to assist with locating the relevant image(s) on the system.
- A log of such requests will be maintained.
- If images of third parties are also shown within the requested images of the person who has made the access request, consideration must be given as to whether there is a need to obscure the images of the third parties.

Access to / Disclosure of CCTV/ANPR Images

The College respects the right of individuals to check the accuracy of any personal data that is being kept about them, either on computer or in a relevant filing system.

Exceptions to the above paragraph are:

- where disclosure would simultaneously disclose data about another person (unless that person consents to the disclosure);

Any Data Subject wishing to gain access to personal data held about them may do so by the submission of a request in writing to the Data Protection Officer (until 25 May 2018, together with the payment of a fee), on each occasion that access is requested. The College aims to comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within 40 calendar days of receipt of the application form until 25 May 2018 and within one month thereafter. Where the College receives large numbers of requests, or especially complex requests, the time limit may be extended by a maximum of two further months.

A copy of the standard request form for "Access to Personal Information" is available on the College website: http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/subject-access-requests/

To make a subject access request to see personal data held by the College an 'Application Form for Subject Access' available on the link above will assist the process.

If after consulting the above web page there are still queries, please contact the College's Data Protection Officer. Contact details of the College's Data Protection Officer are available on the Legal Services Office webpages.

9. Freedom of Information

As a public body the College may receive requests under the Freedom of Information Act 2000 (FOIA). All such requests are dealt with centrally by the College Secretariat and Communications office.

Section 40 of the FOIA contains a two-part exemption relating to information about individuals. If we receive a request for CCTV footage, we will consider:

- Are the images those of the requester? If so then that information is exempt from the FOIA/FOISA. The request will be treated as a data protection subject access request as explained above.
- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles.

10. Use of the Systems

All Security staff and other authorised personnel must read this Code of Practice prior to being instructed on the operation of the system.

All personnel authorised to use these systems are required to have read and comply with the College's data protection policy which is issued to all operators of College CCTV.

The CCTV system can be used to observe the campuses and areas under surveillance and identify incidents that require a response; the appropriate response will be determined by Security Services staff.

The ANPR system must only be used to identify vehicle number plates and time of access and egress. Note: 'Number Plate' means the display plate of the Vehicle Registration Number (VRN) OR vehicle licence number (foreign registered vehicles).

CCTV surveillance should be in accordance with the stipulated objectives.

Whenever a response is required a log should be commenced on an Imperial College Crime Report.

Viewing monitors are password protected and viewed only by authorised personnel.

Deliberate failure to comply with these procedures may result in disciplinary proceedings being taken.

Requests for information and complaints

Complaints received in relation to the use of the CCTV and ANPR systems should be made to the Head of the Security Department. He or she will investigate the allegation or complaint and then follow the normal College Grievance procedures outlined on the College's HR website.

Complaints in relation to the disclosure or image supply should be made in writing to the Head of the Security Department.

The Head of the Security Department can provide further information on the systems upon request.

The address for further information and complaint regarding **CCTV** and **ANPR** is:

Head of the Security Department , Level 1, Sherfield Building, South Kensington Campus, London SW7 2AZ. Tel: 020 7594 9550.

The College's Data Protection Officer may also assist with information and complaints; contact details of the College's Data Protection Officer are available on the Legal Services Office webpage: http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/.

Breaches of data protection should be reported as per the College's breach notification procedure outlined here: http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/data-breaches/ or to the College's Data Protection Officer.

Date for review of Policy: May 2019

Further information:

- College's Data Protection website.
  http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/
- The College's car parking policy is available here, it references the ANPR system which provides for controlled access to authorised vehicles.
  http://www.imperial.ac.uk/estates-facilities/travel/car-parking/car-parking-regulations/