CCTV POLICY

Owner

1. The University has in place a CCTV surveillance system, "the system". The RAUL site comprises for this purpose the Chiswick campus and the Weetwood Hall campus.

2. The Head of Facilities is responsible for the operation of the system and for ensuring compliance with this policy and the procedures documented in the Procedures Manual. They may be contacted as follows:

Head of Facilities

3. Arlene MacManus

   0208 332 8295

   Estates&facilities@richmond.ac.uk

Data Protection Act 2018

4. CCTV digital images, if they show an identifiable individual, are personal data and are covered by the Data Protection Act. This Policy is associated with the RAUL Data Protection Policy, the provisions of which should be always adhered to as well as the ICO CCTV Code of Practice.

The System

5. The system comprises: Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; Public information signs.

6. Cameras will be located at strategic points internally within the campus. No camera will be hidden from view.

7. Signs will be prominently placed at strategic points of the campus to inform staff, students, visitors, contractors, partners, and members of the public that a CCTV installation is in use.

8. Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the System

9. The system has been installed by RAUL with the primary purpose of reducing the threat of crime generally, protecting RAUL's premises and helping to ensure the safety of all RAUL 's staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

    9.1.1. Deter those having criminal intent.

    9.1.2. Assist in the prevention and detection of crime.

    9.1.3. Facilitate the identification, apprehension, and prosecution of offenders in relation to crime and public order.

    9.1.4. Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is or is threatened to be taken.

    9.1.5. In the case of security staff to provide management information relating to employee compliance with contracts of employment

10. The system will not be used:

    10.1.1. To provide recorded images for the world-wide-web.

    10.1.2. To record sound other than in accordance with the policy on covert recording.

    10.1.3. For any automated decision taking

11. Covert recording

    11.1 Covert cameras may be used under the following circumstances on the written authorisation or request of the University Vice President or Head of Student Affairs and where it has been assessed by the Head of Facilities and the University Data Protection Officer.

    11.1.1. That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and

    11.1.2. That there is reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

    11.1.3. Any such covert processing will only be carried out for a limited and reasonable period consistent with the objectives of making the recording and will only relate to the specific suspected unauthorised activity.

11.1.4. 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.

Staff

12. All staff with access to CCTV will be made aware of the sensitivity of handling CCTV images and recordings. The Head of Facilities will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

13. Training in the requirements of the Data Protection Act 2018 will be given to all those required to work in the system by the Data Protection Officer.

14. Due to open nature of reception desk. Images captured by the system are not always monitored in real time.

15. If the system is actively monitored by someone with appropriate access this should be done in a private space.

16. Only the Head of Facilities, Assistant Facilities Manager and Security Supervisor have access to CCTV footage.

17. When CCTV footage needs to be reviewed after an incident it is done so in a private space such as the Facilities tech room or a private meeting room.

18. No unauthorised access to the facilities tech room will be permitted without approval from the Head of Facilities, Assistant Facilities Manager or Security Supervisor

Administration and Procedures

19. Details of the administrative procedures which apply will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

20. Images of identifiable living individuals are subject to the provisions of the Data Protection Act 2018; the Head of Facilities is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

Recording

21. Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.

22. Images will normally be retained for eighteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard

drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

23. All hard drives and recorders shall remain the property of RAUL until disposal and destruction.

24. Where the images are required for longer storage in association with Incident Reporting, this will be done securely and with the report and retained for a maximum of 3 years (after the incident is concluded) in alignment with the Limitation Act 1980.

Access to Images

25. All access to images will be recorded in the Access Log as specified in the Procedures Manual.

26. Access to images will be restricted to those staff who need to have access in accordance with the purposes of the system as above.

27. Access to images by third parties

27.1 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 authorities:

27.1.1. Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.

27.1.2. Prosecution agencies

27.1.3. Relevant legal representatives

27.1.4. The media where the assistance of the public is required in the identification of a victim of crime or the identification of a perpetrator of a crime.

27.1.5. People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.

27.1.6. Emergency services in connection with the investigation of an accident.

28. Access to images by a subject

28.1 CCTV digital images, if they show a recognisable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by C.C.T.V. is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

28.1.1. A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Data Protection Officer. Subject Access Request Forms should be requested from the University Data Protection Officer.

28.1.2. The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data or ask anyone else for a copy of the data. All communications must go through the RAUL Data Protection Officer. A response will be provided promptly and in any event within thirty days of receiving the request and information, unless an extension to this time is applicable and justified.

28.1.3. The Data Protection Act gives the Data Protection Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

28.1.4. All such requests will be referred by the Data Protection Officer.

28.1.5. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

29. Where the University does not control the CCTV system but requires access to the content for any of the reasons in this policy, they will have in place an appropriate agreement with the CCTV provider to gain access to content as required and in accordance with this clause 6.

Request to Prevent Processing

30. An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

31. All such requests should be addressed in the first instance to the Head of Facilities or the Data Protection Officer, who will provide a written response within 30 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

Complaints

32. It is recognised that members of RAUL and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Head of Facilities. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke RAUL 's Centralised

Complaints Procedure by obtaining and completing a RAUL Complaints Form and a copy of the procedure. Complaints forms may be obtained from the University.

33. These rights do not alter the existing rights of members of RAUL or others under any relevant grievance or disciplinary procedures.

Compliance Monitoring

34. The contact point for members of RAUL or members of the public wishing to enquire about the system will be the Head of Facilities at above contact details.

35. Upon request enquirers will be provided with:

    35.1 A summary of this statement of policy

    35.2 An access request form if required or requested.

    35.3 A subject access request form if required or requested.

    35.4 A copy of the RAUL central complaints procedures.

36. All documented procedures will be kept under review and an annual report made to the Estates & Facilities committee and Operations Committee

37. The effectiveness of the system in meeting its purposes will be kept under review and reports submitted annually to the Estates & Facilities committee and Operations Committee.

38. Where a change to the CCTV system technology or processing is proposed, an ad hoc Data Protection Impact Assessment will be completed by the Data Protection Officer and presented to the IT & Data Governance Committee and/or Operations Committee.

VERSION MANAGEMENT

Responsible Department: Estates & Facilities			
Approving Body: University Board (on recommendation of Operations Committee)			
Version no.	**Key Changes**	**Date of Approval**	**Date of Effect**
1	Updated to reflect CP move and incorporate Leeds	14 March 2024	April 2024
2	Formatted and reapproved for 2025-26 AY	24 July 2025	September 2025
	Restricted Access? ***Tick as appropriate*: Yes ☐ No x**		