CCTV Policy

Mark Kennell

Head of Community Safety and Security

Contents

1. Introduction

1.1 The University of Warwick uses a Closed-Circuit Television (CCTV) surveillance system to reduce and deter crime and to help provide a safe and secure environment for students, staff and visitors, and to protect University property.

1.2 This policy sets out the accepted use and management of surveillance equipment and recorded images to ensure that the University complies with its legal obligations under the UK GDPR, the Data Protection Act 2018, the Human Rights Act 1998 and the Freedom of Information Act 2000.

1.3 The University has produced this policy in line with the Information Commissioner's CCTV Code of Practice.

1.4 The University is not subject to the Surveillance Camera Commissioner's Surveillance Camera Code of Practice, or the European Data Protection Board's guidelines 2/2019 on processing of personal data through video devices, but has taken these documents into account in the preparation of this policy as a matter of good practice.

1.5 This policy should be read together with the University's other policies including the University Information Management Policy Framework and its health and safety policies.

1.6 The policy aims to ensure data protection by design and by default. Surveillance images are actively monitored and recorded, and used in accordance with this policy.

2. Scope of this policy

2.1 This policy applies to all of the University's closed-circuit television (**CCTV**) systems including:

(a) Main campus CCTV system

(b) the Automatic Number Plate Recognition (**ANPR**) cameras

(c) Body-Worn Video cameras (**BWV**)

(d) unmanned aerial vehicles (**UAV**)

(e) Wellesbourne Campus

2.2 For the avoidance of doubt, this policy does not apply to:

(a) any webcam or audio-visual systems located in meeting rooms or lecture theatres

(b) dashboard cameras installed in University vehicles

(c) the use of any surveillance equipment as part of the University's core education and research functions (e.g. cameras used as part of a research study, time-lapse cameras installed to monitor the progress of construction projects, etc.), or

(d) temporary installations in relation to major events (e.g. the Commonwealth Games) where surveillance is installed on the University's campus on a short-term basis as part of national security or counter-terrorism measures.

2.3 This policy applies to the surveillance systems listed in paragraph 2.1 above in all parts of the University's campuses. This includes the locations listed below where locally controlled standalone CCTV systems are in operation. Whilst they are part of the central University system, any access to images by the Community Safety team, or other internal department involved in investigations such as Student Discipline, is achieved through a formal request via Info Compliance to the hosting department:

(a) the University of Warwick Science Park

(b) the Islamic Prayer Hall

(c) Computer Sciences.

2.4 This policy applies to fixed and portable surveillance cameras.

3. Principles

3.1 The University is subject to the General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

3.2 Due regard is given to the Data Protection Principles embodied in GDPR. These principles require that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date;

(e) kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

3.3 Due regard is given to the Surveillance Camera Commissioner's Guiding Principles:

(a) 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.

(b) 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.

(c) 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.

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

(e) 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.

(f) 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.

(g) 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.

(h) 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.

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

(j) 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.

(k) 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.

(l) 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.

4. Purposes of the surveillance systems

4.1 The systems are intended to provide an increased level of security in the University environment for the benefit of those who study, work, live in, or visit the campus.

4.2 The University only uses surveillance where it is necessary and proportionate in response to the purposes set out below.

4.3 The University will consider alternatives to the use of surveillance and only use surveillance where it is the most appropriate means to address the purposes set out below.

4.4 The surveillance systems will be used to monitor and collect visual images for the purposes of:

(a) the prevention and detection of crime,

(b) the identification, apprehension and prosecution of offenders,

(c) the prevention, detection and response to all forms of anti-social behaviour (including harassment and public disorder),

(d) supporting and monitoring compliance with the University's health and safety obligations, and creating a safer University community,

(e) supporting and monitoring compliance with the University's parking regulations,

(f) supporting and monitoring compliance with the University's Regulations and other policies,

(g) gathering evidence by a fair and accountable method for use in investigations relating to the above matters, and

(h) improving the operational response of security patrols and providing assistance to emergency services.

4.5 By way of example (but without limitation), relevant criminal offences are likely to include offences against the person and offences against property.

4.6 The surveillance systems and all recorded material (and copyright in the same) are owned by the University. Recorded material will not be sold, used for commercial purposes, used for entertainment or used to provide information or material for research purposes.

4.7 The use of surveillance will be conducted in a professional, ethical and legal manner and any footage will not be used for purposes not set out in this policy.

5. CCTV systems

Installation

5.1 Cameras will be sited so that they only capture images relevant to the purposes for which they are installed and following the completion of an Operational Requirement document and Data Protection Impact Assessment to justify the installation.

5.2 The Operational Requirement document will function as a design document and make sure that the installation of cameras is rationalised.

5.3 Before the installation of CCTV, consideration must be given to an assessment of the appropriateness of and the reasons behind the installation of CCTV in that location, and these considerations must be documented.

5.4 All CCTV installations must be carried out by a University-approved installer and with the approval of the Head of Community Safety and Security or their nominated representative. This establishes rigour around the process to ensure that CCTV equipment is procured and installed in an appropriate, cost-effective way, and that new equipment can be integrated with the existing systems.

5.5 Equipment must be carefully positioned to:

(a) cover the specific area to be monitored only,

(b) minimise privacy intrusion,

(c) ensure that recordings are 'fit for purpose' and not in any way obstructed, so far as reasonably practicable (e.g. by foliage, etc.), and

(d) minimise the risk of damage or theft, or the commission of anti-social behaviour (e.g. vandalism in relation to the equipment).

5.6 Cameras should be sited as assessed in the Operational Requirement document. Cameras are only located so that they capture images relevant to the purpose for which the system was set up.

5.7 CCTV cameras are not installed in areas in which individuals would have an expectation of privacy, such as toilets and changing rooms.

5.8 CCTV cameras at the University cover the following spaces in generic terms:

(a) academic buildings

(b) accommodation blocks

(c) administrative and logistics buildings

(d) car parks, and

(e) publicly-accessible locations (e.g. conference centres, the bus interchange, the Piazza, etc.).

5.9 Every effort is made to position cameras so that their coverage is restricted to the University's property, which includes outdoor areas. The CCTV system will have privacy screening functionality.

5.10 The CCTV system will continuously record activities in the area of coverage.

5.11 A limited number of cameras are capable of audio recording (e.g. the Foyer at the Community Safety Hub and the individual BWV cameras). Facial recognition software is built into some parts of the system; however, the University does not use the capability at this moment in time, nor does it see the requirement to do so in the near future. A separate DPIA assessment and notification to the campus community will be made should the need arise.

Maintenance

5.12 An appropriate maintenance programme should be in place for all devices, which is managed by the University's Estates department's contract management team. Maintenance is required on all hardware components of the CCTV system, including cameras, cabling, recording devices/servers, monitors and associated ancillary equipment, as well as software and firmware, which is updated on a regular basis.

5.13 Maintenance of the University's main CCTV system is outsourced pursuant to a commercial contract, save for the Body Worn Video system (cameras, recording equipment, pc and software, firmware and security patches) that is managed and maintained by the Community Safety team under the terms of a separate commercial agreement.

Staff

5.14 The CCTV system is operated by the University's Community Safety team whose personnel are employed directly by the University.

5.15 The Control Room is staffed 24-hours a day by qualified and Security Industry Authority (SIA) licensed staff working in shifts. All systems are recording 24-hours a day, but not all are monitored 24/7 due to the number of cameras on site.

5.16 All staff involved in the operation of the system will, by training and access to this policy, be made aware of the sensitivity of handling CCTV images and recordings. The training includes making staff aware of the potential criminal offences associated with misuse of personal data, how to recognise a data subject access request, information sharing with the police, and compliance with the University's information management policies.

5.17 The Community Safety team will audit local departmental CCTV annually if necessary, against this policy and concerns regarding the application for the Data Protection Act or other legislation will be referred to the Legal and Compliance Services department.

5.18 Disciplinary action may be taken, up to and including dismissal, against any member of staff found to have breached the policy or is found to have misused the CCTV system beyond its intended purpose.

Security of the CCTV Control Room

5.19 Access to the Control Room and recorded/live footage will be prohibited except to authorised staff, who are required to sign into and out of the facility on entry and exit.

5.20 Visitors to the CCTV control room will be permitted with the authorisation of the Head of Community Safety and Security or their nominated representative. Visitors may include officers from law enforcement agencies or regulators. Anyone requesting access into the Control Room does so only when necessary to carry out their duties.

5.21 All visitors to the Control Room will be required to sign the visitor's book and a declaration of confidentiality. Any such visits will be conducted and recorded in accordance with the CCTV operator's manual.

5.22 Other personnel admitted to the Control Room e.g. cleaning staff, engineers and IT staff carrying out repairs must be authorised by the Head of Community Safety and Security or their representative and must be supervised at all times whilst there.

5.23 In the event of a major incident arising, such as serious public disorder, bomb threats/explosions or serious fires, the police will be given authority to enter and take an active role in the use of Control Room facilities and functions. Such authority will be given by the Head of Community Safety and Security or nominated representative.

5.24 All access to the medium on which the images are recorded will be documented and approved by Legal and Compliance Services.

Retention and disposal

5.25 Recorded CCTV footage will be retained for 31 days after which time it will be automatically written over, thereby deleting it.

5.26 CCTV footage will be retained for a longer period in cases where a copy has been made in relation to a police investigation or is required for evidential purposes.

5.27 In the event of the recorded footage being required for evidence or the investigation of crime, it will be retained for a further 90 days, or until it is no longer required for those purposes, or any investigation has been completed.

5.28 The disposal of footage will take place in accordance with the University's Information and Records Management Policy and the University Records Retention Schedule.

6. Automatic Number Plate Recognition (ANPR) systems

6.1 The University uses ANPR for Occupancy Reporting, Traffic Management and Green Travel Plan Support. ANPR is also installed in some car parks to ensure compliance with the University's Parking Regulations e.g., regarding payment for parking.

6.2 These cameras are controlled and operated by a third-party supplier (APCOA Parking UK Ltd) under contract, separately to the University's main system.

6.3 The APCOA Parkway System retains granular entry/exit data which is used to create a visit history and list of contraventions. The information captured on the system include plate patch image, date and time of entry and exit. The following details are captured for all vehicles passing through the ANPR zone:

a) Overview image of the vehicle

b) Vehicle Registration

c) Time of Entry/ Exit

d) Date of Entry/ Exit

6.4 All maintenance costs for the equipment hardware will be covered under an equipment warranty period enabling repair or replacement for part failure for a period of 24 months post installation. After this period, cost for replacing faulty or obsolete equipment will be borne by the University under the terms agreed in the commercial contract. Software and firmware upgrades and security patches should be included within the terms of the maintenance agreement under commercial contract.

6.5 APCOA provide University enforcement staff with appropriate first line training at commencement and refreshers as needed directly from the equipment manufacturers.

6.6 Any faults alerted via the back-office systems for ANPR and payment terminals will be assessed by the local Control Room staff to establish if first line or second line maintenance is needed.

6.7 Any first line maintenance requirements will be alerted to the University's transport officers whereas second line maintenance requirements will be notified to the University equipment suppliers for resolution within agreed timescales.

6.8 The transport officers will have access to a fault reporting module on their handheld devices to raise a fault report for second line maintenance needs directly to APCOA.

6.9 To ensure the longevity of equipment, we propose to provide front line maintenance training for the UOW Team and devise a programme of actions aligned to the manufacture's guidance.

6.10 APCOA will also provide 1 x annual planned maintenance visit on all ANPR cameras, barriers, intercoms and pay stations so to maximise the longevity of all hardware on campus

6.11 The still images are used for parking enforcement purposes only. Only APCOA Parking UK Ltd and their camera supplier, Jenoptic, will have access to the cameras for maintenance, set-up, and support.

6.12 The ANPR system has default data retention settings of:

a) 3-month auto-deletion of all images
b) 2 years for Vehicle Registration Number (VRN) data

6.13 Data within the APCOA Parkway system is set to auto-delete every 3 months. Data held within the back-office system is auto-deleted every 6 weeks from the last point of action.

6.14 Parking charge notices that progress to debt stage are retained as active cases for a year. VRN data is held for 2 years.

6.15 This policy should be read alongside the University's car park terms and conditions and parking and traffic policy.

7. Body Worn Video (BWV) systems

7.1 The BWV system comprises of personal-issue cameras with in-built audio recording capability worn by the University's Community Safety officers in the course of their normal duties, and the associated hardware, docking station and Reveal DEMS software https://www.revealmedia.co.uk/products/dems-360 to operate the system.

7.2 BWV cameras are issued as part of an officer's personal protective equipment (**PPE**).

7.3 Maintenance of the BWV system is included within 'Maintenance' (5.13 above)

7.4 BWV will only be activated for the purposes set out in this policy, for example:

(a) where officers believe that they are entering a conflict situation,

(b) during the conduct of searches for illicit drugs, or

(c) where there is a requirement to record audio and video images so that an accurate and detailed account of a conversation or incident is recorded for evidential purposes.

7.5 A verbal declaration is made at the start of any recording so that those being recorded are aware of the recording. Where possible, the declaration is repeated if additional people are captured by the BWV.

7.6 If individuals object to the recording, the officer will consider these objections and determine whether or not they outweigh the reasons for recording. The officer will communicate their decision to the objector.

7.7 When activated by an officer to record, the BWV system will have automatically recorded the previous 30 seconds prior to the camera being activated. This enables the evidential trail to be extended to a time before an officer engaged in an incident and will provide images and audio of everything leading up to the officer activating the camera.

7.8 Footage is uploaded automatically when an officer places their camera into the proprietary docking station via the Reveal DEMS software. All footage is encrypted and not able to be edited by an officer to ensure a complete and accurate audit trail of the footage for evidential purposes.

7.9 The footage is downloaded onto a University server via the Reveal docking station and controlled by the Reveal DEMS software.

7.10 BWV cameras are always retained within the Community Safety Hub within the secure personal locker of each officer when the officer is not on shift.

7.11 Footage is automatically deleted from the server after a period of 31 days.

7.12 As well as providing the opportunity to record evidential material of an incident, the use of BWV can also enable increased scrutiny of officers' actions and the decisions taken by them.

7.13 Officers wear signage (i.e., a badge / light) indicating that they are wearing BWV and an LED indicator light shows when the camera is recording.

8. Unmanned Aerial Vehicle (UAV/drone) systems

8.1 The University uses UAV/drone equipment with on-board cameras to conduct building surveys and for marketing purposes (e.g., to take promotional images of the campus).

8.2 The University does not use UAV systems for surveillance purposes; however, it acknowledges that images of individuals may be captured during the course of the activities mentioned in paragraph 8.1 above.

8.3 It is unlikely that individuals will be identifiable from images collected by UAV systems and these images will not constitute personal data.

8.4 The use of UAV/drone systems is covered by the University's Drone Policy and Procedures, managed by Estates.

9. Access to surveillance footage

Freedom of Information Act and GDPR Data Subject Rights requests

9.1 The Freedom of Information Act and the UK GDPR will be adhered to in relation to requests for access to surveillance footage.

9.2 Requests by individual data subjects for images relating to themselves "Subject Access Request" should be in writing by completing a Data Subject Rights Request Form and submitting this to the University's Legal and Compliance Team together with proof of identification. Further details of this process are detailed on the University's Legal and Compliance webpage: Data Protection - Security & Information Management - Warwick

9.3 Any request for access to information must be made to Legal and Compliance Services, who maintain a log of requests and respond to them. Consideration is given to the need to redact / obscure footage.

9.4 Where the Legal and Compliance team is unable to comply with a Subject Access Request without disclosing the personal data of another individual who is identified or identifiable from that information, it is not obliged to comply with the request unless satisfied that the individual has provided their express consent to the disclosure, or if it is reasonable, having regard to the circumstances, to comply without the consent of the individual.

Requests for Information from law enforcement agencies

9.5 Requests for access to information from the police and other law enforcement agencies must be made to Legal and Compliance Services, who maintain a log of requests and respond to them. Consideration is given to the need to redact/obscure footage.

9.6 Requests submitted by the police should include the signature and name in block capitals of an officer of the minimum rank of inspector and reasonable detail to justify the request.

9.7 Requests from the police not containing an explanation for the request must contain the signature of an officer of the minimum rank of superintendent.

9.8 The University will exercise its judgment on a case-by-case basis in determining whether to provide access to information in response to a request from the police.

Requests for information from other parts of the University

9.9 Requests to view surveillance, for instance in relation to contractors, a member of staff or student disciplinary investigations, should be made to Legal and Compliance Services clearly setting out why the request is being made, how it will assist the investigation, and how it relates to the purposes set out in this policy.

9.10 The Head of Community Safety and Security (or their nominated representative) may provide access to CCTV images, having consulted with Legal and Compliance Services, to Investigating Officers when sought as evidence in relation to student discipline cases.

Reporting crimes to the police and information sharing in emergencies

9.11 The Community Safety team may access and share footage without consultation with Legal and Compliance Services in emergencies where it is vital that the footage is made available immediately. The Head of Community Safety and Security will notify Legal and Compliance Services of these emergency situations as soon as reasonably practicable, and the recipient of the footage will formalise their request in writing retroactively. Such an example might include where there is an immediate threat to life.

9.12 The Community Safety team will notify law enforcement agencies and ask them to investigate any matter recorded by the surveillance system which is deemed to be of a criminal nature, in accordance with the purposes set out in this policy.

9.13 Footage may be disclosed in other circumstances in order to comply with a legal obligation (e.g. a court order) or where an exemption in the UK GDPR applies.

10. Transparency

10.1 A copy of this policy will be published on the University's website.

10.2 The University's core privacy notices published on its website will provide information on the use of surveillance cameras. These privacy notices contain, amongst other things, details of the University's registration with the Information Commissioner's Office and contact details for its Data Protection Officer.

10.3 The University will clearly display signage in accordance with guidance issued by the Information Commissioner's Office, so that staff, students and visitors are aware they are entering an area covered by surveillance. The signs indicate:

(a) the presence of monitoring and recording,

(b) the purpose of monitoring and recording,

(c) hours of operation,

(d) the ownership of the system, and

(e) contact telephone numbers for complaints and queries.

10.4 Signs are placed in all locations where surveillance is used e.g., at main pedestrian walkways, around accommodation blocks, and car park entrances.

11. Complaints

11.1 The University's complaints procedure is available online.

11.2 Any complaint concerning misuse of a surveillance system will be treated seriously and investigated by the Head of Community Safety and Security or their nominated representative with assistance from Legal and Compliance Services.

11.3 The Head of Community Safety and Security or their nominated representative will ensure that every complaint is acknowledged in writing within seven working days. The acknowledgement will include information about the complaint procedure to be undertaken.

11.4 Misuse of a surveillance system will be handled in accordance with the University's disciplinary procedure.

11.5 If a person is unhappy with the University's response to a request that they have made for access to surveillance footage under either the Freedom of Information Act or the UK GDPR, they may be entitled to an internal review of the University's response. Details on how to request an internal review will be set out in the response itself.

11.6 If a person remains unhappy, they have the right to complain to the Information Commissioner's Office.

12. Covert Recording

12.1 The University may only undertake covert recording with the written authorisation of the Director of Legal and Compliance Services, and at the request of the Head of Community Safety and Security or their nominated representative.

12.2 Covert recording can only be undertaken where:

(a) informing the individual(s) concerned that recording is taking place would seriously prejudice the reason for making the recording; and

(b) there is good cause to suspect that an illegal or unauthorised action(s) is/are taking place or about to take place and the use of CCTV systems to detect such activity is justified,

12.3 Any such monitoring will only be carried out for a limited and reasonable amount of time consistent with the objectives of the monitoring and only for a specific illegal or unauthorised activity. All such occasions will be fully documented via a legitimate interest assessment showing when and why the decision to use covert monitoring was made.

13. Review

13.1 This policy will be reviewed annually by the Head of Community Safety and Security, along with Legal and Compliance Services, who will consider compliance rates and whether the use of surveillance remains justified.

13.2 As part of the review, the Head of Community Safety and Security will consider:

(a) whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation;
(b) the monitoring operation, e.g. if 24-hour monitoring in all camera locations is necessary, or whether there is a case for reducing monitoring hours;
(c) whether there are alternative and less intrusive methods to achieve the stated purposes.

13.3 Systems, which are deemed non-compliant with this policy following a review, must be made compliant within a specified period or must be decommissioned.

13.4 The University's use of surveillance may be subject to audit in the same way as any of the University's other functions.

13.5 Departments must not, under any circumstances install CCTV equipment without consulting and obtaining approval from the Head of Community Safety and Security, or their nominated representative.