University of Kent CCTV Policy

1. Introduction

1.1. This document details the operating policy and standards for the management of Closed Circuit Television (CCTV) installed at the University of Kent Canterbury and Medway campuses in accordance with the requirements of the Data Protection Act (1998) and the CCTV Code of Practice issued by the Information Commissioners Office. The CCTV systems in use at the University of Kent are registered as part of the University's entry on the Data Protection Register held by the Information Commissioner. The University of Kent Data Protection Officer is responsible for this registration.

2. Purpose and Objectives of the System

2.1. The CCTV system has been installed with the intention of reducing crime and the fear of crime the benefit of the campus communities, consistent with respect for individual privacy. These objectives will be achieved by operational usage of the system to:

2.1.1. Assist in the prevention and detection of crime.

2.1.2. Facilitate the identification, apprehension and prosecution of offenders in relation to crime either through the criminal justice system or through disciplinary processes internal to the University of Kent.

2.1.3. To facilitate car parking and traffic management operations.

3. Operating Principles

3.1. The CCTV system will be operated 24 hours a day each day of the year, and the Canterbury Security Control Room will be staffed for this same period.

3.2. To ensure compliance with the Data Protection Act, personal data, including images recorded on CCTV systems will at all times be processed following these principles:

3.2.1. Data will be processed fairly and lawfully.

3.2.2. Data will be processed for a limited purpose and not in any manner not compatible with the purpose of the system.

3.2.3. Data storage will be adequate, accurate, relevant and not excessive.

3.2.4. Data will not be kept for longer than is necessary.

3.2.5. Data will be processed in accordance with individual's rights.

3.2.6. Data will be kept secure.

4. System Description

4.1. The CCTV systems installed in and around the University of Kent campuses comprises a mixture of fixed position cameras and pan/tilt/zoom cameras both at internal and external locations.

4.2. Most cameras on the Canterbury campus are fed back to the central Security Control Room where images are recorded on digital hard disk, and are capable of 24/7 live monitoring by Control Room Operators. Images are recorded for no more than 28 days, at which point the CCTV software will automatically overwrite the earliest recordings. These cameras are linked to the Security Control Room via a dedicated and secure fibre optic network to ensure unauthorised third parties are not able to intercept images.

4.3. Cameras on the Medway campus are fed back to a secure digital server in the Drill Hall Library where images are recorded on a digital hard disk. Recorded images are retained on the hard disc for a period not exceeding 28 days at which point the images are automatically overwritten with new images. The images are capable of live monitoring by the Security Co-ordinator in an office behind the main reception, where screens are positioned to prevent unauthorised users overlooking the footage.

4.4. At some locations CCTV images are fed to local hard disk recorders at the location where the CCTV is installed rather than to the Security Control Room. In these instances the recorders are stored in a locked cabinet in a locked service area, with access to these locations restricted to Security personnel. Data recorded on these local hard disks is saved for a period of no more than 28 days at which time the data is automatically deleted by being overwritten with new footage. There is no capability for live viewing of these local systems.

4.5. The positioning of cameras provides fields of view encompassing entrances to buildings, internal communal areas, other high risk internal locations and public external areas. Examples of high risk areas will be rooms containing high value equipment such as computer servers or valuable artwork etc.

5. Monitoring of CCTV Images

5.1. Live viewing of CCTV on the Canterbury campus will ordinarily be through a feed into the Security Control Room where University of Kent employed Control Room Operators have direct access to monitor the footage. Control Room Operators will undertake training in the CCTV system and the relevant legislation, the Information Commissioners Code of Practice and other policy before undertaking such duties.

5.2. Access to the Security Control Room is limited to authorised personnel only. Those persons automatically authorised will be University of Kent Security staff and Estates Department senior managers.

5.3. Consideration will be given on a case by case basis to other persons requesting access to the Security Control Room by the Head of Security or in their absence the Security Duty Manager balancing any operational need to enter the Control Room with the need to restrict access to sensitive data. This may include for example, service engineers working on Control Room equipment or Police Officers making enquiries. The Control Room

Operator will record any such person entering the Security Control Room under signature in a locally held visitor's log which will record:

5.3.1. Date and time of entry and leaving the Security Control Room
5.3.2. Name and department or organisation
5.3.3. Name of the person authorising their entry
5.3.4. The reason why access was facilitated

5.4. Live viewing of CCTV on the Medway campus will be through a live feed to the Security Co-ordinators office, and access to the live images will be restricted to the Security staff and the Estates Managers with overall responsibility for security of the campus.

5.5. In some circumstances access may be given to authorised persons other than Security staff to monitor live feeds at locations other than the Security Control Room. Those persons authorised will be an employee or person acting on the behalf of the University of Kent who has operational responsibility for the prevention, investigation or detection of crime in their specific area of responsibility. In these circumstances access will be for live viewing only, and these persons will not be authorised to review recorded footage which will be accessed only by authorised Security staff for the purposes listed below. Live feeds in these circumstances should be located in a secure environment to ensure unauthorised persons are not able to view the footage.

6. Use of Covert CCTV

6.1. Ordinarily CCTV camera surveillance will be overt, with clear signage and clearly identifiable cameras. In rare and exceptional circumstances where there is significant reason to suspect that criminal activity is taking place and that overt camera usage would prejudice any investigation into this criminal activity, covert CCTV cameras may be used. The University of Kent Executive Group delegates authority to the Director of Estates to make the final decision to use covert CCTV once an impact assessment has been completed by the University Security Manager which will consider:

6.1.1. If the situation is an exceptional circumstance and there is significant reason to suspect criminal activity.
6.1.2. Whether there is any alternative less intrusive means of investigation other than covert CCTV.
6.1.3. Would the investigation be prejudiced by making it known that cameras were being used in the investigation?
6.1.4. The location and positioning of any CCTV camera taking into account the security of personal data (images) recorded by any device to ensure images are controlled and not accessible to 3rd parties, together with individual rights to privacy.
6.1.5. The specific timeframe any covert camera should be installed to ensure the exceptional usage is proportionate and not excessive.
6.1.6. Whether the use of CCTV in the circumstances is proportionate to the legitimate aim.

6.2. If there is any reason to suspect University of Kent staff involvement in the exceptional circumstance where criminal activity is reasonably suspected of taking place, or where use of covert CCTV may impact a member of staff, the Head of Security will gain the authorisation, under signature from a Human Resources Department Manager before requesting authority to proceed from the Director of Estates.

6.3. A senior manager responsible for the area of the campus in question will also be consulted prior to the positioning of any covert device.

6.4. Images recorded by any authorised covert device will be processed in accordance with all other CCTV data under this policy including retention, access and disclosure principles detailed below. Installation of hard wired cameras will be installed by the nominated CCTV contractor.

7. Body Worn Video Recorders

7.1. Front line operational staff with enforcement responsibilities may be issued whilst on duty with a personal body worn video device. These are small but clearly identifiable mobile CCTV recording devices designed to enhance the personal safety of individuals likely to be called on to deal with potentially volatile situations and/or to record crime scene evidence.

7.2. Images and sound are recorded onto an encrypted HD memory card, and transferred to the Security Control Room where recordings may be burnt to a CD and processed in line with the operational procedures for CCTV evidence including retention, access and disclosure principles detailed below. Any footage recorded on the device which does not fall within the stated purpose and objectives of this CCTV policy (such as accidental recordings caused by user error) will be securely deleted without delay. The decision to delete footage of this nature will be made by the Duty Control Room Operator, and a record will be kept which will detail: the time and date of the footage, the user of the device and the reason for the secure deletion.

7.3. Front line operational staff issued with a body worn video device will only make recordings when presented with volatile or aggressive behaviour, to record the commission of a crime in progress or to record the scene of a crime which has recently occurred. The member of staff will issue a verbal warning to any persons being recorded on the device that video recording is taking place.

7.4. Before being issued with a body worn video device operational staff will undergo training in use of the device together with relevant Data Protection Act, Information Commissioners Code of Practice and policy implications.

8. Processing CCTV Images

8.1. Recorded CCTV footage will be stored on digital hard discs. Access to recorded footage on the system will be limited to University of Kent authorised security personnel. Any reviewing of recorded images will be in accordance with the stated purpose of the CCTV system. A log will be maintained locally in the Security Control Room/Medway Security Co-ordinators office recording any reviewing of footage which will include:

8.1.1. Person reviewing the recorded footage
8.1.2. Time date and location of footage being reviewed
8.1.3. Purpose of reviewing the recordings

8.2. The digital hard discs on which recordings are made will store images for a period of no more than 28 days, at which time the recordings will be automatically overwritten with new footage. In certain circumstances in order to preserve CCTV footage, recordings may be transferred to a CD. This will be limited to circumstances where evidence has been identified on the CCTV footage which is intended to be used to facilitate the identification or prosecution of offenders or assist with internal disciplinary proceedings where there is reasonable suspicion of criminal activity. The decision to burn footage in accordance with this principle will be made by the Head of Security or Security Duty Manager, and a record will be kept in the Security Control Room/Medway Security Co-Ordinators office which will detail who the person making the decision to burn footage was, and the justification for doing so.

8.3. The transfer of images from hard disc to CD will be processed by the Duty Security Control Room Operator in the presence of a witness. Two copies will be made of any footage downloaded to CD: a master copy to be held securely in the Security Control Room, and a working copy for operational usage. All footage downloaded to CD will be recorded in locally held files and the CD's will be marked with indelible ink with the following information:

8.3.1. Name and signature of the Control Room Operator burning the footage to CD.
8.3.2. Name and signature of the person witnessing the process.
8.3.3. Local disk reference number.
8.3.4. Date the CD was created.
8.3.5. Date, times and camera numbers of the footage included on the disk.

8.4. Footage downloaded to CD will be kept in a locked restricted access safe in the Security Office and will be securely destroyed, and a record kept of their destruction, when the footage is no longer needed for prosecution or internal disciplinary purposes or when 12 months has lapsed, whichever is sooner. Disclosure of and access to footage downloaded to CD will be in accordance with the principles listed below in section 11.

9. Quality of Recorded Images

9.1. Images produced by the recording equipment must be as clear as possible in order that they are effective for the purpose for which they were intended. The standards to be met under the Information Commissioners Code of Practice are:

9.1.1. Recording features such as the location of the camera and time and date reference must be accurate and maintained.

9.1.2. Cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.

9.1.3. Consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas.

9.1.4. Cameras must be properly maintained and serviced to ensure that clear images are recorded and a log of all maintenance activities kept.

9.1.5. As far as practical, cameras must be protected from vandalism in order to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit with vandal resistant casing.

10. Appropriate Signage

10.1. Appropriate signage will be displayed at entrances to the campus and the entrances to buildings with CCTV installed so that all persons using the campus for any reason will be aware that they are entering an area which is covered by CCTV. The signs will:

10.1.1. Be clearly visible, legible and be of a size appropriate to the circumstances.

10.1.2. Contain the name of the Data Controller (University of Kent Data Protection Officer)

10.1.3. State the purpose of the CCTV system

10.1.4. Include a contact telephone number for any enquiries

11. Access to Recorded Images

11.1. University of Kent Security Staff.

11.1.1. Access to recorded images for the purposes of reviewing footage to establish if any evidence has been captured on the CCTV system will be restricted to University Security Staff and the Police where necessary. The review will first be authorised by a Security Duty Manager who will ensure:

11.1.1.1. The reason for the review is consistent with the stated purpose and objectives of the CCTV system.

11.1.1.2. A record of the review is kept detailing the time span, specific cameras reviewed, person completing the review and any evidence gathered.

11.1.2. Random footage will be reviewed by the University Head of Security at least once every 28 days to monitor compliance with this policy, the Data Protection Act and the Information Commissioners Code of Practice.

11.2. Data Subject Access Requests

11.2.1. For the purposes of the Data Protection Act recorded images will be considered personal data and data subjects (i.e. persons whose images have been recorded on the CCTV system) have rights under the act, including the right to be informed that personal data is being recorded and the right to view such data. Data subjects requiring access to their personal data should contact the University Data Protection Officer at the Registry, and complete a Subject Access Request form enclosing the relevant fee (currently £10). CCTV footage used for the purposes of internal disciplinary hearings shall not be subject to this Subject Access Request fee,

11.2.2. On receipt of the Subject Access Request, the University Data Protection Officer will advise the University Head of Security whether any disclosure of data should take place. If deemed appropriate the University Head of Security will:

11.2.2.1. With the information supplied by the data subject, ascertain whether the subject has been recorded on any CCTV footage.

11.2.2.2. Establish whether any third parties also recorded on any relevant footage need to be eliminated (by editing or blurring of their faces through software) to protect their rights as data subjects.

11.2.2.3. Supply the data to the data subject on a CD under signature within 40 days or other time as specified by the Data Protection Act.

11.3. Third Party access requests

11.3.1. Third parties (who are not data subjects) who wish to have access to or a copy of recorded CCTV images do not have an automatic right under the Data Protection Act to such disclosure, and as such care must be taken to ensure that neither the Act nor this policy are breached. Third party requests will only be considered in the following categories:

11.3.1.1. Law enforcement

11.3.1.1.1. Copies of recorded images will be supplied to the Police when their request is in pursuit of an investigation into a crime. Requests will be supported by a Section 29 Data Protection Disclosure form which will be signed by a senior Police Officer (Inspector rank or above) and detail the purposes of the request, before any data is disclosed. A copy of this request will be sent to the University Data Protection Officer.

11.3.1.1.2. The Security Control Room Operator will be satisfied that the purposes of the request are related to a crime and that failure to release the images would prejudice the Police investigation and will record in local files (together with the signed Section 29 Disclosure form)the following information:

11.3.1.1.2.1. The date and time copies of images burnt to CD were handed over to the care and control of the Police.

11.3.1.1.2.2. The name and force number of the Police Officer the data was given to.

11.3.1.1.2.3. Details of the CCTV data being disclosed to include the local CD reference number(s).

11.3.1.1.2.4. The Police crime or incident number to which the incident/crime refers.

11.3.1.1.2.5. The signature of the Police Officer collecting the CD(s) to confirm they have received the data images.

11.3.1.2. University Managers

11.3.1.2.1. University Managers charged with the responsibility of staff and/or student disciplinary investigations and hearings may require copies of CCTV to support those investigations and hearings. In these circumstances the nature of the investigation or hearing must be in accordance with the stated purpose and objectives of this CCTV system.

11.3.1.2.2. Requests of this nature should be made by Human Resources Managers or College Masters only, and will be authorised by the University Head of Security. Before disclosing any data the University Head of Security will be satisfied that the request is related to the stated purposes and objectives of the CCTV system as stated in section 2 of this policy.

11.3.1.2.3. If authorised, copies of the relevant CCTV footage will be downloaded to CD in accordance with this policy, and will be signed for by the authorised University Manager, and returned to the Security Office when no longer required for operational use for destruction in line with the policy above.

11.3.1.3. Freedom of Information

11.3.1.3.1. CCTV images are considered personal information and as such would not be disclosed in relation to a Freedom of Information request as this would be considered unfair processing in contravention of the Data Protection Act.

11.3.1.4. Other Third Parties

11.3.1.4.1. Any third party requests for CCTV data which do not fall in to the above two categories (such as legal representatives of data subjects) will be considered on a case by case basis by the University Head of Security who will consult with the University Data Protection Officer before making any disclosure in a manner consistent with data subject access requests outlined above

12. Monitoring and Compliance

12.1. An annual assessment will be conducted by the University Head of Security to evaluate the effectiveness and justification for the continued use of the CCTV system in use at the University of Kent, and assess its compliance with the Data Protection Act and the CCTV Code of Practice issued by the Information Commissioners Office. The results of this report will be assessed against the stated purpose and objectives of the system in this policy. If the scheme is deemed in this report to not be achieving the stated purpose and objectives then remedial action will be taken to modify the systems in use.

12.2. The University Head of Security will also access random footage of recorded images at least once every 28 days to monitor compliance of this Policy, the Data Protection Act and the Information Commissioners Code of Practice. These checks will be recorded and will also include a check to ensure processes and procedures contained in this policy to safeguard privacy and security of data are being adhered to.

12.3. At the start of each shift, the Duty Control Room Operator will complete and record a check on the operational status of the CCTV system to include:

12.3.1. Verifying that the time and date stamp on recorded images is accurate.
12.3.2. Verifying that all cameras are recording correctly and are fully serviceable, reporting defects to the nominated contractors without delay.
12.3.3. Establish that the quality of images being recorded is good.

13. Complaints

13.1. Any complaints relating to the CCTV system should be directed in writing in the first instance to the University Head of Security. Complaints relating to the data protection principles should be directed in writing to the University Data Protection Officer. Once the complaint has been received in writing the University Head of Security or Data Protection Officer will respond to the complaint within 28 days. Records of all complaints regarding the CCTV system together with any follow up action will be maintained by the relevant office. If a person making a complaint is still unsatisfied with the response given, they may appeal the response to the Director of Estates or if the complainant is a member of staff or a student at the University of Kent they may use the policies in existence for raising a formal grievance.

13.2. Contact the University Head of Security: Telephone 01227 823829. Address: Estates Department, Park Wood Road, University of Kent, Canterbury.

Policy Approved By: JSNCC & Staff Policy
Date: 28 May 2014 & 20 June 2014
Review date: January 2018

Version	Date	Control Reason
1.0	June 2014	Document issued and live
1.1	January 2017	All references to previous security roles amended to reflect changes.
	January 2018	(Review pended following appointment of Intern to undertake CCTV policies and practices review and assessment of both against ICO, Surveillance Commissioner's guidelines, and GDPR.)