Privacy Impact Assessment 2019 V4.

Location of surveillance camera system being assessed	University of Kent; Canterbury and Medway Campus
Date of assessment	22/02/19
Review date	22/02/19
Name of person responsible	Mark Arnold, Head of Security
Name of Data Protection Officer	Jordan Hall, Head of Data Protection

1. What are the problems that you need to address in defining your purpose for using the surveillance camera system?

The University of Kent faces a number of key challenges in relation to the management of security and safety, such as

- Large open campuses, with significant number of students, staff and members of the public having access visiting the campus regularly
- Large number of students resident on these campuses
- Venues offering the sale of alcohol are located on campus
- Ensuring the continued security of academic buildings in which sensitive materials and assets are stored
- Providing the physical security element of the Information Security Management system across the university's establishments

The University of Kent has a duty of care to its staff, students and to members of the public who may access its campuses. An operational CCTV system is a proportionate response to the associated challenges of the factors listed above and in facilitating the university in meeting its wider legal obligation. In addition, the use of CCTV will also allow the university to establish, exercise and defend and its own legal rights and claims.

2. Can surveillance camera technology realistically mitigate the risks attached to those problems?

The use of surveillance camera technology can mitigate those risks because

- It is an established and effective method for ensuring the safety of staff, students and visitors
- That the existence of the system is in and of itself a deterrent against crime and as such protects buildings and assets from damage, disruption and vandalism
- The system can be used to support the investigation and detection of crime or reports of crime, as well as any investigation of safety and security related incidents
- Provide law enforcement bodies (or the university itself) with any evidence which may lead to possible criminal, civil or disciplinary action either against staff, students or members of the public
- CCTV records can be used to assist in the effective resolution of disputes
- Can be used for the effective management of traffic on campus

3. What other less privacy-intrusive solutions such as improved lighting have been considered?

The University of Kent maintains a dedicated campus security team, who are ultimately responsible for providing the security function at the University. As part of their wider work, they conduct regular patrols, providing a security presence when needed, they also are responsible for responding to security incidents on campus. The team are the main point of contact for enforcement authorities around wider public order and crime issues. The CCTV system is designed to complement these activities and provide a greater oversight of the security landscape, thereby making the most of the resources available to the team.

4. What is the lawful basis for using the surveillance camera system? State which lawful basis for processing set out in Article 6 of the GDPR or under Part 3 of DPA 2018 applies when you process the personal data that will be captured through your surveillance camera system.

The processing of surveillance camera data is in the legitimate interests of the university, its students and staff as well as members of the public accessing our campuses. This is because the proper monitoring and processing of data captured by CCTV systems forms part of the university's overarching efforts to meet its duty of care obligations. In addition, the processing of such information is in the legitimate interests of the data subjects themselves, who will reasonable expect the university to provide for them a safe and secure environment whilst they are on campus. The data protection rights of data subjects involved are safeguarded by the processes and controls that the university has in place.

5. Can you describe the information flows?

- Live viewing of CCTV on the Canterbury campus will ordinarily be through a feed into the security control room. CCTV is monitored in the security control room at the University's campus in Canterbury 24 hours a day, every day of the year. The University shall ensure that live feeds from CCTV and Surveillance Systems are only viewed by authorised personnel from the University's security staff and Estates department senior managers or members of staff approved by the Head of Security whose role requires them to have access to such Data. Recorded images will only be viewed in designated, secure offices.
- Recorded CCTV will be stored on secure university servers, with access restricted to control room staff and the Head of Security.
- In certain circumstances in order to preserve recordings captured on CCTV or Surveillance Systems, the Head of Security may direct that recordings captured on CCTV or Surveillance Systems be transferred to CD (or another service medium) to achieve the purposes and objectives for which CCTV or Surveillance Systems are installed. The transfer of any such recording to CD (or other service medium) will be processed by the duty security control room operator in the presence of a witness. The process is detailed in Part 8 of the CCTV policy.

6. What are the views of those who will be under surveillance?

The University CCTV Policy and this PIA will be submitted to the JNCC committee for comment, any further Data Protection concerns raised during that process will be addressed through amendment to the DPIA.

7. What are the benefits to be gained from using surveillance cameras?

- The University will be able to maintain more accurate data around incidents that occur on campus
- The University will be more effective in safeguarding the welfare of its staff and students
- By utilising real time monitoring the university will be able alert authorities of evolving risks to students/staff/the public
- The overt nature of the cameras will act as a deterrent and provide safety assurances to those on campus

8. What are the privacy risks arising from this surveillance camera system? State the main privacy risks relating to this particular system. For example, who is being recorded; will it only be subjects of interests? How long will recordings be retained? Will they be shared? What are the expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective? What is your assessment of both the likelihood and the severity of any impact on individuals?

- Risk of intrusion into the private life of data subjects captured whist on campus- through careful siting of cameras (in public areas of the campus) as well as display of signage the risk of such intrusion will should be minimised. The processing of data will be completed in a secure environment, subject to a number of safeguards contained in the CCTV policy and any subsequent sharing will be proportionate and limited to the lawful purpose being relied upon. There are established data breach processes, so that should any of the controls fail, the effect of a breach on any data subject will be managed and minimised.

9. Have any data protection by design and default features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements? State the privacy enhancing techniques and other features that have been identified, considered and accepted or rejected. For example, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy masking on cameras that overlook residential properties? If these have not been adopted, provide a reason.

- Non-evidential material will be retained for 28 days only, and subsequently erased.
- Camera locations are chosen to minimise viewing of spaces not relevant to the legitimate purpose of the monitoring
- Should there be any amendments to policy or additions to the system, the DPIA will be reviewed and any risks around intrusion/privacy will be addressed.
- Images produced by CCTV and Surveillance Systems are as clear as possible in order that they are effective for the purpose for which they were intended. CCTV and Surveillance Systems are subject to regular maintenance
- Access to the security control room and primary monitoring facilities are limited to authorised personnel from the University's security staff and Estates department senior managers. Control Room Operators have unique and individual log in details and access is therefore controlled and audited on this basis
- Staff using CCTV or Surveillance Systems are given appropriate training to ensure they understand and observe the legal requirements related to the Processing of relevant Data. In addition, all university staff are required to complete the University's GDPR and data protection training, which outlines their obligations around reporting data breaches.

- The Data generated by CCTV and Surveillance Systems is stored on University servers. The University BWV camera data is stored using a cloud computing system. The University IS Dept. has ensured that all reasonable steps have been taken to maintain the security of its information. The University is Cyber Essentials certified.

10. What organisations will be using the surveillance camera images, and where is the controller responsibility under the GDPR and Data Protection Act 2018? List the organisation(s) that will use the data derived from the camera system and identify their responsibilities, giving the name of the data controller(s) and any data processors. Specify any data sharing agreements you have with these organisations.

- Law enforcement agencies- controller to controller
- Further, restricted sharing of information with third party local authorities under the Kent and Medway Data Sharing agreement (where a lawful reason applies)- controller to controller
- Data Subjects perusing claims for damages against third parties
- When disclosure ordered by a Court

The University of Kent will not routinely share CCTV recording with others and will only share such data where there is a lawful basis for so doing. The University of Kent may disclose data derived from the CCTV system to legal professionals, in order to obtain advice and defend/pursue legal action.

11. Do the images need to be able to recognise or identify individuals, or could the purpose be met using images in which individuals cannot be identified? Explain why images that can recognise or identify people are necessary in practice. For example, cameras deployed for the purpose of ensuring traffic flows freely in a town centre may not need to be capable of capturing images of identifiable individuals, whereas cameras justified on the basis of dealing with problems reflected in assessments showing the current crime hotspots may need to capture images in which individuals can be identified.

It is imperative as to ensure the accuracy of any subsequent processing that the system captures high quality data, to the extent that any person can be idenfited. The quality of any data will also enable the university to more effectively meet the legitimate interests of those involved.

12. How will you inform people that they are under surveillance and respond to any Subject Access Requests, the exercise of any other rights of data subjects, complaints or requests for information?

- Data Subjects may make a request for disclosure of Personal Data which may include CCTV images (a "**Data Subject Access Request**"). A Data Subject Access Request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with the University's subject access policy at *https://www.kent.ac.uk/infocompliance/dp/access-requests.html*

- In order for the University to locate relevant footage, any requests for copies of recorded images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the Data Subject.

- The University reserves the right to obscure images of third parties when disclosing recordings captured on CCTV or Surveillance Systems when responding to a Data Subject Access Request once the technology is available at the University.

- Any request for recorded images other than by way of a Data Subject Access Request will be considered under the Freedom of Information Act 2000 (an "**FOIA Request**"). An FOIA Request is subject to the statutory conditions from time to time in place and should be made in writing, in accordance with the University's policy at *https://www.kent.ac.uk/infocompliance/foi/request.html*

- On receipt of a Data Subject Access Request or FOIA Request, the University Data Protection Officer shall advise the University Head of Security whether any disclosure should be made.

- The DPO and Head of Security will ensure that an up to date privacy notice is published on the Estates webpages.
- Body worn video cameras or mobile recording devices are clearly identifiable and any images or sound recorded are encrypted. Prior to initiating any recording using a body worn video camera or mobile recording device, University staff will warn any persons being recorded or Data Subjects that video and sound recording is being initiated. Staff will record the date, time, and location and reason for any recording made using a body worn video camera or mobile recording devices.

13. How will you know if the particular camera system/hardware/software/firmware being considered does deliver the desired benefits now and in the future? It

The Head of Security and the DPO will, on an annual basis, review this DPIA, CCTV asset register and the CCTV policy to ensure that the controls and measures in place continue to be effective and that use of CCTV remains aligned to our lawful condition for processing such data. The DPO will monitor any cloud based storage facility for GDPR compliance.

14. What future demands may arise for wider use of images and how will these be addressed?

There are currently no plans to introduce any further functionality to the system as part of any future development of the system. However, should the University of Kent establish a legitimate need to implement any new technology, the Head of Security and DPO will ensure the concept of Privacy by design and default is an essential factor in the scoping and commissioning of any subsequent work and this DPIA will be updated accordingly.

15. Have you considered the extent to which your surveillance camera system may interfere with the rights and freedoms conferred under the European Convention on Human Rights?

The University of Kent has policy and procedures which align with the Surveillance Camera Code of Practice and the ICO Data Protection Code of Practice for Surveillance cameras. As such, the ECHR rights and freedoms have been addressed by design and are evident in the controls and measures implemented during the operational delivery of the CCTV system.

16. Do any of these measures discriminate against any particular sections of the community?

No

17. Does the Data Controller maintain an asset register of security cameras including details around locations, types and capabilities of the camera that are currently in use?

Yes- in the form of separate datasets

Approval

Measures approved by:

Date:

Are there any residual risks? What mitigations will be put in place to reduce these risks? Please detail:

Residual risks approved by:

Date:

DPO advice:

Summary of DPO advice and whether processing can proceed:

This DPIA was written in collaboration with the DPO and as such any mitigation of identified risks were addressed in the drafting of this document.

Name: Jordan Hall

Date: 22/02/19

DPO advice accepted or overruled *Delete as appropriate*

If overruled, you must explain your reasons

Name:

Date:

Information Flows

Optional questions to help describe the collection, use and deletion of personal data. It may also be useful to refer to a flow diagram or another way of explaining data flows.

5.1 How is information collected?

CCTV camera X	Body Worn Video X
Unmanned aerial systems (drones)	Stand-alone cameras
ANPR X	Real time monitoring
Other (please specify)	

5.2 Does the system's technology enable recording?

Yes- CCTV data from both campuses will be recorded and stored in a secure building with restricted access. BMV will only be recorded when initiated by the operative and only in circumstances specified in the policy. BWV will be uploaded to cloud based storage on docking on.

5.3 What type of transmission is used for the installation subject of this PIA (tick multiple options if necessary)

Fibre optic: Canterbury	Wireless (please specify below)
Hard wired (apart from fibre optic, Broadband please specify) Other (please specify)	Other: Medway On University network with encrypted firewall.

5.4 What security features are there to protect transmission data e.g. encryption (please specify)

CCTV data is on an encrypted and closed fibre optic network.

BWV data is held in a cloud based system and the data is transmitted by secure internet connection.

5.5 Where will the information be collected from?

Public places (please specify) X	Car parks Buildings/premises (external) X
Buildings/premises (internal public areas) X	Other (please specify)

5.6 From whom/what is the information collected?

General public in monitored areas (general observation) X	Vehicles
Target individuals or activities (suspicious persons/incidents	Visitors X
Other (please specify) Students and Staff	

5.7 What measures are in place to mitigate the risk of cyber-attacks which interrupt service or lead to the unauthorised disclosure of images and information?

The university certified as complying the Government Cyber Essentials standards around managing a secure network and associated Information Management System.

5.8 How is the information used? (tick multiple options if necessary)

Monitored in real time to detect and respond to unlawful activities X	Monitored in real time to track suspicious persons/activity X
Compared with reference data of persons of interest through Automatic Facial Recognition software	Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
Used to search for vulnerable persons X	Used to search for wanted persons
Recorded data disclosed to authorised agencies to support post incident investigation by, including law enforcement agencies X	Recorded data disclosed to authorised agencies to provide intelligence X
Other (please specify)	

5.9 How long is footage stored? (please state retention period)

28 days. This can be longer in certain circumstances as set out in the University CCTV policy or other authorised University data retention policies e.g. *https://www.kent.ac.uk/human-resources/privacystatement/index.html*.

5.10 Retention Procedure

System operator required to initiate deletion/ deletes automatically? Under certain circumstances authorised persons may override the retention period e.g. retained for prosecution as detailed in the University CCTV policy

5.11 With which external agencies/bodies is the information/footage shared?

Statutory prosecution agencies X	Judicial system X
Local Government agencies X	Data subjects

Legal representatives X	Other (please specify); The University is a signatory of the Kent and Medway Information Sharing Partnership. In limited circumstances with Trade Union representatives as per the CCTV policy.

5.12 How is the information disclosed to the authorised agencies

Only by onsite visiting	Copies of the footage released to those mentioned above X Please see CCTV policy for procedure
Offsite from remote server X For body worn cameras only	Other (please specify)

5.13 Is there a written policy specifying the following? (tick multiple boxes if applicable)

The University operate CCTV in line with the requirements made I the University CCTV Policy. This policy sets out how information is disclosed, including requests for information (by data subjects and third parties). The policy also sets out how the University will operationalise the Surveillance Camera Commissioner's Code of Conduct as well as best practice as issued by the ICO.

5.14 Do operating staff receive appropriate training to include the following?

Legislation issues X	Monitoring, handling, disclosing, storage, deletion of information X
Disciplinary procedures X	Incident procedures X
Limits on system uses X	Other (please specify)

5.15 Do CCTV operators receive ongoing training?

Yes

5.16 Are there appropriate signs which inform the public when they are in an area covered by surveillance camera systems?

Yes