Version number: 1.0
Policy owner: Head of Campus and Residential Services
Effective date: 01/12/2018
Review date: 01/12/2019
Equality Analysis Toolkit: 01/03/2019

CCTV Policy

1. Policy Statement

1.1. We believe that CCTV and other surveillance systems have a legitimate role to play in helping to maintain a safe and secure environment for all our students, staff and visitors. However, we recognise that this may raise concerns about the effect on individuals and their privacy. This policy is intended to address such concerns.

1.2. Images recorded by surveillance systems may contain personal data which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring that the legal rights of students, staff and visitors relating to their personal data, are recognised and respected.

1.3. This policy is intended to assist staff in complying with their own legal obligations when working with personal data. In certain circumstances, misuse of information generated by CCTV or other surveillance systems could constitute a criminal offence.

2. Definitions

2.1. For the purposes of this policy, the following terms have the following meanings:

2.1.1. **CCTV** means fixed and domed cameras designed to capture and record images of individuals and property. This also includes security body worn cameras that capture sound and vision.

2.1.2. **Data** is information which is stored electronically, or in certain paper-based filing systems. In respect of CCTV, this generally means video images. It may also include static pictures such as printed screen shots.

2.1.3. **Data subjects** means all living individuals about whom we hold personal information as a result of the operation of our CCTV (or other surveillance systems).

2.1.4. **Personal data** means data relating to a living individual who can be identified from that data (or other data in our possession). This will include video images of identifiable individuals.

2.1.5. **Data controllers** are the people who, or organisations which, determine the manner in which any personal data is processed. They are responsible for establishing practices and policies to ensure compliance with the law. [We are the data controller of all personal data used in our business for our own.]

2.1.6. **Data users** are those of our employees whose work involves processing personal data. This will include those whose duties are to operate CCTV cameras and other surveillance systems to record, monitor, store, retrieve and delete images. Data users must protect the data they handle in accordance with this policy and our Data Protection Policy.

2.1.7. **Data processors** are any person or organisation that is not a data user (or other employee of a data controller) that processes data on our behalf and in accordance with our instructions (for example, a supplier which handles data on our behalf).

2.1.8. **Processing** is any activity which involves the use of data. It includes obtaining, recording or holding data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing or destroying it. Processing also includes transferring personal data to third parties.

2.1.9. **Surveillance systems** means any devices or systems designed to monitor or record images of individuals or information relating to individuals. The term includes CCTV systems as well as any technology that may be introduced in the future such as automatic number plate recognition (ANPR), body worn cameras, unmanned aerial systems and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

3. About this Policy

3.1. We currently use CCTV cameras to view and record individuals on and around University premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice. This policy also explains how to make a subject access request in respect of personal data created by CCTV.

3.2. We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3. This policy covers all employees (academic and professional services), students, consultants, contractors, freelancers, volunteers, interns, casual workers, and agency workers and may also be relevant to visiting members of the public.

3.4. This policy is non-contractual and does not form part of the terms and conditions of any employment or other contract. We may amend this policy at any time without consultation and the policy will be regularly reviewed to ensure that it meets legal requirements and relevant guidance published by the ICO and industry standards.

3.5. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4. Personnel Responsible

4.1. The Director of Estate Management has overall responsibility for ensuring compliance with relevant legislation and the effective operation of this policy. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to The Head of Campus and Residential Services. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of Campus Services Manager.

4.2. Responsibility for keeping this policy up to date has been delegated to the Head of Campus and Residential Services.

5. Reasons for the use of CCTV

5.1. We currently use CCTV around our sites as outlined below. We believe that such use is necessary for legitimate business purposes, including:

5.1.1. to prevent crime and protect buildings and assets from damage, disruption, vandalism and other crime;

5.1.2. for the personal safety of students, staff, visitors and other members of the public and to act as a deterrent against crime;

5.1.3. to support law enforcement bodies in the prevention, detection and prosecution of crime;

5.1.4. to assist in day-to-day management, including ensuring the health and safety of staff, students and others;

5.1.5. to assist in the identification of actions that may result in disciplinary proceedings against staff or students or action against contractors providing services to the University;

5.1.6. to promote a safe community environment; and

5.1.7. to assist in traffic management and parking enforcement.

5.2. This list is not exhaustive and other purposes may be or become relevant.

6. Monitoring

6.1. Predominately CCTV monitors the exterior of the buildings and covers entrances and exits to site. The number of cameras is suitably modest and locations have been prioritised to prevent excessive coverage. There are a small number of cameras located internally in key locations for the protection of assets. Halls of Residence have internal cameras which only focus on the main entrance door to the block. Locations of cameras are at Appendix A, but for security reasons are not for publication. No cameras are hidden or covert. Where possible cameras are placed out of risk of criminal damage.

6.2. Cameras are positioned so that they only cover public or shared areas. As far as practically possible no cameras focus directly into private residential areas or offices.

6.3. Surveillance systems, other than body cameras do not record sound.

6.4. Cameras are not actively monitored. Images are recorded 24 hours a day, 7 days a week, 365 days a year. Images will only be examined where there is justification i.e. when investigating an incident, seeking clarification of an event, improving understanding in relation to Health and Safety or performance matters or when a crime has occurred or is suspected. This has been communicated to staff who operate the system.

6.5. Staff using surveillance systems will be given appropriate training to ensure they understand and observe the legal requirements related to the processing of relevant data.

7. How we will operate any CCTV

7.1. We will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of the organisation operating the system, the purpose for using the surveillance system and who to contact for further information, where these things are not obvious to those being monitored.

7.2. Live feeds from CCTV cameras will only be monitored where this is reasonably necessary, for example to protect health and safety.

7.3. We will ensure that live feeds from cameras and recorded images are only viewed by approved members of staff whose role requires them to have access to such data. Recorded images will only be viewed in designated, secure offices.

7.4. In exceptional circumstances contracted security officer may use body worn cameras that capture both sound and vision.

8. Use of data gathered by CCTV

8.1. In order to ensure that the rights of individuals recorded by the CCTV system are protected, we will ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

8.2. At the request of the Police, other agency or a third party, a nominated officer may review the recorded footage from the CCTV system to establish whether an incident was captured by any of the cameras.

8.3. The nominated officer may then advise the third party making the enquiry whether the incident has been captured and recorded on the system. They will not, at this stage, indicate to the third party the specific nature of what has been recorded.

8.4. Should the Police, an agency or a third party wish to view footage relating to an incident they must complete an Image Removal Form (see Appendix B). This will require the approval of one off the nominated officers. The same procedure applies for requests of duplicate copies.

8.5. Nominated officers have been informed of the procedures to follow in relation to law enforcement, subject and third party requests. Critically, they know not to deviate from this policy and not to disclose information to others unless it is explicitly permitted.

8.6. Once information has been disclosed to the Police they become the Data Controller for the purposes of data protection legislation.

9. Retention and erasure of data gathered by CCTV

9.1. Data recorded by the CCTV system will be stored on the system's hard drive. The data is stored for 31 days when it is automatically overwritten and so permanently deleted. Images retained for the purpose of investigation may be retained for a longer period of time. Exactly how long images will be retained for will vary according to the purpose for which they are being recorded. For example, where images are being recorded for crime prevention purposes, data will be kept long enough only for incidents to come to light. All data will be permanently deleted once it is no longer useful for the purpose to which it was retained. Any data that is retained will be logged so as to keep a record; an example log appears at Appendix B.

9.2. At the end of their useful life, all digital information stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

9.3. Any footage recorded by security officers using body worn cameras will be downloaded to a memory card. This would be securely stored in a locked safe until it can be transported to their Head Office where it will be transferred to a secure encrypted storage device. Data will be permanently deleted after 31 days if not passed to relevant authorities.

10. Use of additional surveillance systems

10.1. Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, we will carefully consider if they are appropriate by carrying out a Data Protection Impact Assessment (DPIA).

10.2. A DPIA is intended to assist us in deciding whether new surveillance cameras are necessary and proportionate in the circumstances and whether they should be used at all or whether any limitations should be placed on their use.

10.3. Any DPIA will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

10.4. No surveillance cameras will be placed in areas where there is an expectation of privacy (for example, in changing rooms) unless, in very exceptional circumstances, it is judged by us to be necessary to deal with very serious concerns.

11. Covert monitoring

11.1. We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or extremely serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

11.2. In the unlikely event that covert monitoring is considered to be justified, it will only be carried out with the express authorisation of The Vice Chancellor's Group. The decision to carry out covert monitoring will be fully documented and will set out how the decision to use covert means was reached and by whom. The risk of intrusion on innocent staff and students will always be a primary consideration in reaching any such decision.

11.3. Only limited numbers of people will be involved in any covert monitoring.

11.4. Covert monitoring will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected illegal or unauthorised activity.

12. Ongoing review of CCTV use

12.1. We will ensure that the ongoing use of existing CCTV cameras in the workplace is reviewed at least every 12 months to ensure that their use remains necessary and appropriate, and that any surveillance system is continuing to address the needs that justified its introduction. We will maintain a log of such reviews for audit purposes.

13. Requests for disclosure

13.1. We may share data with third parties where we consider that this is reasonably necessary for any of the legitimate purposes set out above in paragraph 5.2.

13.2. No images from our CCTV cameras will be disclosed to any third party, without express permission being given by Head of Campus and Residential Services. Data will not normally

be released unless satisfactory evidence that it is required for legal proceedings or under a court order has been produced.

13.3. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime.

13.4. We will maintain a record of all disclosures of CCTV footage.

13.5. No images from CCTV will ever be posted online or disclosed to the media.

14. Subject Access Requests

14.1. Data subjects may make a request for disclosure of their personal information and this may include CCTV images (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 our subject access policy which can be found at https://www.chi.ac.uk/about-us/policies-and-statements/data-protection

14.2. In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

14.3. We reserve the right to obscure images of third parties when disclosing CCTV data as part of a subject access request, where we consider it necessary to do so.

15. Complaints

15.1. If any member of staff has questions about this policy or any concerns about our use of CCTV, then they should speak to Head of Campus and Residential Services in the first instance.

15.2. Where this is not appropriate or matters cannot be resolved informally, employees should use our formal grievance procedure.

16. Requests to prevent processing

16.1. We recognise that, in rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact the University Data Protection Officer dpofficer@chi.ac.uk.

APPENDIX B: CCTV Retention Log

Date Data Retained	Date of Data Captured	Time from – to	Reason for retention	Authorised by	Storage Method	Outcome	Date of Data Deletion	Method of Deletion	Name of Staff	Signature