CCTV Code of Practice

Harper Adams University

April 2020

Table of Contents

1. Introduction

a. Harper Adams University is the owner of a public closed circuit television system (CCTV) currently installed on the Campus and in/on University buildings off Campus; body worn and covert cameras are also incorporated for special events.

b. Cameras are located in various areas internally and externally around the campus and off campus including:-

   i. Car Parks

   ii. Academic building

   iii. Service buildings

   iv. Bars

   v. Student Union

   vi. Accommodation

   vii. Shops

c. There are several types of camera –

   i. Overt fixed – these record uncontrolled images e.g. Post room, doors etc.

   ii. Overt Pan, Tilt, Zoom (PTZ) – these are controllable cameras that can follow vehicles or subjects when required.

   iii. Covert cameras will only be used with the authority of a SMT member in order to help resolve a criminal matter.

   iv. Body worn/Head Cam used by security at special events when dealing with drunkenness, violence and anti-social behaviour. They will also be used for searches where drug possession or use is suspected or being investigated.

   v. Overt temporary cameras which may be used in areas not covered by fixed CCTV in order to target a specific issue.

d. The cameras cover roadways, car parks, buildings both internal and external including foyers and corridors, vulnerable public facing offices, academic buildings, pavements and thoroughfares, and licensed premises.

e. Images are recorded centrally on servers held under HAU control; they are all viewable centrally by security staff. In addition, a limited number of management staff have the facility to monitor cameras sited within their own areas of responsibility. For example the farm and the biomass buildings.

2. OBJECTIVES FOR THE USE OF CCTV SYSTEMS

a. The objectives for the use of the CCTV system is to:-

i Assist in providing a safe and secure environment for the benefit of those who might visit, work or live on the campus.

ii Reduce the fear of crime by reassuring students, staff and visitors.

iii Deter and detect crime, public disorder and anti-social behaviour.

iv. Identify, apprehend and prosecute offenders in relation to crime, public disorder and anti-social behaviour.

v. Provide the Police, Health and Safety Executive and University with evidence upon which to take criminal, civil and disciplinary action respectively.

vi. Monitor and assist with traffic management.

vii. Assist in the monitoring and deployment of security staff during normal duties and emergency situations.

viii. Protect security officers from undue threats and violence.

3. PROCEDURAL AND ADMINISTRATIVE NOTES

a. The Estates and Facilities Manager of the University retains overall responsibility for the system and delegates the day to day management to the Security Officers. It is the Security and Portering Manager responsibility to ensure that CCTV within the University is managed in line with this Code of Practice at all times.

b. All images produced by the system remain the property and copyright of the University.

c. The University will only investigate images for use in a staff disciplinary case when there is a suspicion of gross misconduct and not to generally monitor staff activity. In these situations the investigating manager or HR Manager/Advisor will formally request access to images from the Security and Portering Manager, where these may prove or disprove suspected potential gross misconduct. Where access is given, the confidentiality of these images and who is able to access them, will be closely controlled.

d. Likewise the images of students behaviour within the accommodation blocks will only be sought as evidence at the discretion of the Head of Student Services or her deputy (or in their absence a member of the SMT)

e. Covert cameras will be only be used on rare occasions when a series of criminal acts have taken place e.g. thefts in the same area not fitted with CCTV. Authority of the University Estates/Facilities Manager will always be sought before installing any covert cameras.

4. SECURITY CONTROL ROOM

a. The Security Control Room is situated in the Main Building next to the Porters Lodge and is capable of receiving images from throughout the campus. The Security office has access restrictions and will be either staffed by University Security Officers or Porter, or will otherwise be secured.

b. The Control Room is also equipped with a Home Office licensed radio system linking the room with uniformed Security Officers who provide mobile and foot patrols of the car parks and are able to respond to incidents identified on the CCTV monitors.

5. DATA PROTECTION

a. This Code of Practice reflects the spirit and guidance issued by the Information Commissioner's Office as documented in the 'CCTV Code of Practice Revised Edition 2017' and will not be used to invade the privacy of any individual, residence, business or other private premises, buildings or land.

b. The University is committed to complying with the requirements of the GDPR and the Data Protection Act 2018 and will operate the system in accordance relevant legislation. The University will include the CCTV system on the University's data protection notification. The Security and Portering Manager will be responsible for ensuring that the notification covers the purposes for which the system is used.

c. The standards, which must be met in order to comply with the relevant legislation are:

Personal data shall be:

i. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

ii. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; *(there is an exemption around archiving, scientific and statistical purposes)*

iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

iv. accurate and, where necessary, kept up to date;

v. kept for no longer than is necessary

vi. ensure appropriate security of the personal data, using appropriate technical or organisational measures ('integrity and confidentiality').

d. All members of staff involved in operating the system will be made aware of the objectives of the scheme as set out in paragraph 2 of this Code and will be permitted only to use the system to achieve those objectives.

e. All members of staff involved in operating the system will be forwarded a copy of the CCTV Codes of Practice for reference and compliance purposes and will sign to say they have read and understood it. A further copy will be available in the security lodge.

f. The University recognises the importance of strict guidelines in relation to access to and disclosure of recorded images and all members of staff should be aware of the restrictions relating to this set out in this Code and the rights of individuals

under Data Protection Legislation.

6. ADMINISTRATION

a. It will be the responsibility of the Estates/Facilities Manager or Security and Portering Manager or in their absence, his/her deputy to:-

i. Select camera sites and initial areas to be viewed.

ii. Be responsible for compliance with the relevant Data Protection Legislation.

iii. Take responsibility for control of the images and make decisions on how these can be used.

iv. Ensure the system is secure and only viewed by authorised persons*.

v. Ensure that the procedures of this Code of Practice comply with the current CCTV Codes of Practice produced by the Information Commissioner's Office.

vi. Introduce a CCTV incident log and record of Police or other Statutory Authority requests for images.

vii. Ensure adequate signing is erected.

viii. Regularly evaluate the system to ensure it complies with the latest legislation, CCTV Codes of Practice and its use is in accordance with these Codes of Practice.

* Authorised persons include: -

i. Security staff.

ii. Head of Student Services.

iii. Management staff with a legitimate reason for accessing images – e.g. managers/HR investigating the potential gross misconduct of staff.

iv. Police Officers.

v. Other Statutory Offices e.g. Health and Safety Executive Officers.

vi. Members of staff facing disciplinary action and Trade Union officials representing them.

vii. Students facing disciplinary action and their friends or representatives.

b. It will be the responsibility of the Security and Portering Manager to:-

i. Clearly communicate the specific purposes of the recording of and use of images and objectives to all security staff.

ii. Ensure that a CCTV incident log and record of Police or other Statutory Authority requests for images is maintained.

iii. Carry out annual audits to check that procedures are being complied with.

iv. Ensure that the audit team includes CCTV practices and procedures on their regular audits of the Security Services Department.

v. Ensure that regular 3 monthly reviews are conducted of all locked images and delete those not still required for evidential purposes.

vi. Ensure that all Data Protection Act forms received from the Police or other investigatory bodies e.g. Health and Safety Executive are filed for future reference.

vii. Ensure that all data and images are erased after a period of 3 months unless locked or retained for evidential purposes.

c. It will be the responsibility of the individual security officer to :-

i. Select appropriate images to be recorded on controllable cameras (Pan-Tilt-Zoom PTZ) so as to comply with the objectives outlined above.

ii. Ensure that targeting of individuals with the cameras is only conducted when there is reasonable suspicion that the person falls within one of the objectives set above e.g. committing a criminal offence.

iii. Not to view into private property and be mindful of student privacy within student accommodation.

iv. Complete the CCTV incident log as appropriate.

7. STORING AND VIEWING IMAGES

a. Following a major refurbishment, most of the images recorded on the University cameras are digitally stored, on the University's servers. There are a few older cameras that are still recording to local hard drives.

b. In the event of the Police requiring images they can be 'burnt' onto a CD/DVD for evidence in court, on receipt of the appropriate receipt of a Data Protection Form.

c. In general CCTV images will be retained for a period of 14 days, after which they will be automatically deleted.

d. Viewing of live images on monitors is restricted to security operators or other authorised person (see paragraph 6 above).

e. Images are generally viewed confidentially in the security office or in other secure private offices or in the case of disciplinaries, may be presented to a selected panel and displayed on screens privately for the panels use.

f. Requests to view images or image disclosure should be made in writing to the Security and Portering Manager.

8. DISCLOSURE

a. The following guidelines will be adhered to in relation to disclosure of images:-

i. Will be in line with the above objectives.

- Will be controlled under the supervision of the Security and Portering Manager or his/her deputy.

ii. A log book will be maintained itemising the date, time(s), camera, person copying, person receiving and reason for the disclosure.

iii. The appropriate disclosure documentation from the Police will be filed for future reference.

iv. Images must not be forwarded to the media for entertainment purposes or be placed on the internet.

v. Images will only be released to the media for identification purposes in liaison with the Police of other law enforcement agency.

NB: Even if a system was not established to prevent and detect crime, it would still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

b. Any other requests for images should be routed via the Security and Portering Manager or his/her Deputy, as disclosure of these may be unfair to the individuals concerned. In some limited circumstances, it may be appropriate to release images

to a third party, where their needs outweigh those of the individuals whose images are recorded.

i. Example: A member of the public request's CCTV footage of a car park, which shows their car being damaged. They say they need it so that they or their insurance company can take legal action. You should consider whether their request is genuine and whether there is any risk to the safety of other people involved.

c. The University has discretion to refuse any third party request for information unless there is an overriding legal obligation such as a court order or information access rights. Once an image has been disclosed to another body, such as the police, then they become the data controller for their copy of that image. It is their responsibility to comply with the Data Protection Act (DPA) in relation to any further disclosures.

9. SIGNAGE

a. Signage has been erected at the main entrances to the University Campus and at other locations where CCTV is in use informing them that CCTV surveillance is in operation.

b. The signs contain details of the University and a contact number for security.

c. It is the responsibility of the Security and Portering Manager to ensure adequate signing is erected to comply with the Information Commissioner's Code of Practice.

10. SUBJECT ACCESS REQUESTS

a. Individuals whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images. All such requests are handled by the Security and Portering Manager.

i. These images must be provided within one month of receiving a request and the Data Protection Officer must always be informed of all such requests.

ii. Those who request access must provide you with details which allow you to identify them as the subject of the images and also to locate the images on your system.

iii. A log of such request will be maintained in the disclosure log.

iv. If images of third parties are also shown within the images of the person who has made the access request, consideration must be given as to whether

there is need to obscure the images of the third parties. A public space CCTV camera records people walking down the street and going about their ordinary business. Where nothing untoward has occurred, this can be released without editing out third party images.

11. FREEDOM OF INFORMATION

a. As a public body the University may receive requests under the Freedom of Information Act 2000 (FOIA). All such requests are dealt with by the Freedom of Information Officer.

b. The response should be made within 20 working days from receipt of the request.

c. Section 40 of the FOIA and Section 38 of the FOISA contain a two-part exemption relating to information about individuals. If you receive a request for CCTV footage, you should consider:-

   i. Are the images those of the requester? If so, then that information is exempt from the FOIA/FOISA. Instead this request should be treated as a data protection subject access request as explained above.

   ii. Are the images of other people? These can be disclosed, only if disclosing the information in question does not breach data protection legislation.

12. USE OF THE SYSTEM

a. All security staff and other authorised users* must read these Codes of Practice prior to being instructed on the operation of the system.

b. The live CCTV system can be used to observe the Campus and other areas under surveillance and to identify incidents that require a response. The response should be proportionate to the incident being witnessed. On some occasions the intervention of a security officer may be sufficient on other occasions contacting the Police to respond may be the appropriate action.

c. Such surveillance should be in accordance with the stipulated objectives.

d. Whenever a response is required, a log should be commenced and a Security Report completed.

e. Viewing monitors should be switched off when not in use to prevent unauthorised us or viewing.

* Authorised users – see paragraph 6 above.

13. COMPLAINTS

a. Complaints received in relation to the use of the CCTV system should be made to the Estates and Facilities Manager/ Security and Portering Manager who will investigate the allegation or complaint and then follow the normal University grievance procedures as outlined on the Human Resources website.

b. Complaints in relation to the disclosure or image supply should be made in writing to the Estates and Facilities Manager.

14. CHANGES TO THE CODE

a. Any changes to this code will only take place after consultation with the Students Union.

b. The changes will then have to be ratified by the University Estates and Facilities Manager.

David Harding

Security and Portering Manager

April 2020