The University of Huddersfield

Code of Practice for the Operation of CCTV

Contents

The Scope of this Code 2

Introduction and accountability 2

Complaints 2

Review, approval and amendments 4

The Code 5

Objectives 5

The System 5

The Security Control Room 6

Security Control Room Administration and Procedures 7

Covert Monitoring 7

Workforce Monitoring 7

Staff 8

Recording and Retaining 8

Monitoring Procedures 9

Digital Recording Procedures 9

Standards 9

Access by Data Subjects 11

Rights of Data Subjects 12

Continuity of evidence 12

APPENDIX I 13

APPENDIX II 14

APPENDIX III 16

APPENDIX IV 17

APPENDIX V 18

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

The Scope of this Code

Introduction and accountability

The University of Huddersfield has installed a comprehensive Closed Circuit Television (**CCTV**) surveillance system (the **System**) whereby cameras have been installed at the campus. Images are monitored by the security staff at the Control Room.

Using software and cameras located within buildings, data will be monitored by nominated staff within the faculty or department whose areas the cameras are designed to protect, as well as Security Control. A list of nominated staff is included at Appendix I of this Policy.

The System is owned by the University and operated by the Estate and Facilities department . The Control Room is staffed by the University's security team, which is comprised of the University's security staff and Contract Security Staff.

This Code is intended to act as guidance for Estates staff, the operators of the System and all members of the University community.

The Code's purpose is to ensure that the System is used to create a safer environment for students, staff and visitors to the University, and to ensure that its operation is consistent with the obligations on the University imposed by the Data Protection Act 1998 (the **Act**). The objectives of the Code are outlined at paragraph 1.1 below. This Code is designed to work with the University's Data Protection Policy, the provisions of which should be adhered to at all times.

Guidance published in 2014 by the Information Commissioner's Office (the **ICO**) on CCTV can be found on the ICO's website or by using the link below:

http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/cctv-code-of-practice.pdf

Complaints

The Security Manager is responsible for the operation of the System, and, in the first instance, for ensuring compliance with this Code. Breaches of the Code by any member of staff may constitute a disciplinary matter under the relevant conditions of employment. It may also be a criminal offence. It is also recognised that other members of the University may have concerns or complaints in respect of the operation of the System. Any concerns in respect of the System's use or regarding compliance with this Code should, in the first instance, be addressed to the Security Manager in writing or by email using the contact details below.

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

Review, approval and amendments

This Code has been approved by Estates and Facilities and is due for review in May 2019.

Contact details:

Security Manager	Maggie Birkinshaw
Security Manager Telephone	01484 472632
Email address	M.Birkinshaw@hud.ac.uk
Security Control Room	01484 472221

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

Code of Practice

1. *Objectives*

1.1 The System has been installed by the University for the principal purposes of preventing and detecting crime. It is recognised, however, that ancillary benefits of operating CCTV for these purposes may include reduction of the fear of crime generally, the provision of a safer public environment for the benefit of those who work within the University or who visit and may assist with increasing the level of customer care. These objectives must, however, be consistent with respect for individuals' privacy.

1.2 The System will be monitored in accordance with these objectives and, accordingly, monitoring will be permitted only to:

- assist in the prevention and detection of crime;
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order and as an aid to public safety;
- assist with the enforcement of University car parking regulations and to assist in the management of the car parks;
- provide and operate the System in a manner which is consistent with respect for the individuals privacy;
- assist with the provision of a safer public environment;
- assist with the promotion of the principles of customer care; and
- assist in work place monitoring where this relates to involvement in criminal activity or gross misconduct.

2. *The System*

2.1 The System is all internet protocol based, password protected and comprises of a selection of fixed position cameras, monitors, recording facilities on designated CCTV University servers and public information signs. The cameras cover building entrances, car parks, perimeters, external areas and internal areas such as receptions, the library recreational spaces and teaching and study areas. They do not cover areas where individuals have a reasonable expectation of privacy, such as toilets and changing rooms.

2.2 The System encompasses Queensgate Campus. It will also include CCTV images that, in due course, are captured by the System and monitored at the twenty-four hour Control Room.

2.3 The System is operational and images are capable of being monitored for twenty-four hours a day, throughout the whole year.

2.4 The University's staff, students and the general public are made aware of the presence of the System and its ownership by compliant University signage prominently placed at the main entrances to and relevant areas on the Campus. This sets out the purposes for processing CCTV images (in accordance with paragraph 1.1 above), and identifies the University as the party responsible for processing those images.

2.5 To ensure privacy, wherever practicable, the cameras are prevented from focusing or dwelling on domestic accommodation and this will be demonstrated on request to local residents. Where domestic areas such as gardens are near those areas which are intended to be covered by the scheme, the Security Manager (or nominee) will consult with the owners of the domestic area to discuss what images may be recorded.

2.6 Images captured on camera are recorded on digital hard drive recording for use in accordance with this Code. Persons monitoring the images at locations other than the Library or the Security Control Room will not be permitted to view anything other than the live stream without the permission of the Security Manager. Any images recorded will be managed by the Security Manager for images recorded in the Security Control Room and by the Director of Computing and Library Services for images recorded in the Library.

2.7 Although every effort has been made in the planning and design of the System to give it maximum effectiveness, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

2.8 For the purposes of the Act, the Data Controller is the University and the University is legally responsible for the management and maintenance of the System.

2.9 In order to comply with the objectives of this Code with regard to public safety (see paragraph 1.1) Control Room staff may monitor University car parks. Monitoring of car parks may also take place in order to assist colleagues with the enforcement of the University car parking regulations and the prevention and detection of crime.

3. The Library

3.1 Images captured by the System in the library shall be monitored by the library wardens during library opening hours.

3.2 The System monitors in the library shall be kept in a secured room with access only granted to those members of staff who need to monitor the system and who have been appropriately trained in accordance with this policy. No unauthorised access shall be permitted at any time.

3.3 Any incidents recorded on the library System shall be recorded by the library wardens on the Incident log maintained by the Security Manager as described in 5.1.

3.4 The designated nominees listed in Annex I shall have the ability to play back and record images captured by the System in the library when strictly necessary. The designated nominees shall be responsible for ensuring that all such downloads are logged on the central register and that all

copies are made in accordance with the requirements of this code of practice and are securely delivered to the Control Room at the earliest possible opportunity and in any event within 24 hours.

4. *The Control Room*

4.1 Images captured by the System will be monitored in the Control Room. The Control Room is a self-contained and secure room. The monitors in the Control Room cannot be seen from outside.

4.2 Access to the Control Room is strictly limited to the Security Manager, Senior Management and staff members specifically authorised by either the Security Manager or Senior Management.

4.3 No unauthorised access to the Control Room is permitted at any time. Police officers and any other person with statutory powers of entry may enter with the explicit consent of the Security Manager or nominee

4.4 Persons other than those specified in paragraph 4.2 may be authorised to enter the Control Room on a case-by-case basis. Written authorisation is required and may only be given by the Security Manager or nominee. Each separate visit will require individual authorisation and will be supervised, at all times, by the Security Manager or nominee. Such visitors will not be given access to any data which falls within the scope of the Act.

4.5 In an emergency and where it is not reasonably practicable to secure prior authorisation, access may only be granted to persons with a legitimate reason to enter the Control Room by the officer on duty at that time. Such access will be recorded.

4.6 Before granting access to the Control Room, officers must satisfy themselves of the identity of any visitor and ensure that the visitor has the appropriate authorisation. All visitors will be required to complete and sign the visitors' log, which shall include their name, their department or the organisation they represent, the person who granted authorisation for their visit (if applicable) and the times of their entry to and exit from the Control Room. A similar record shall be kept of the officer on duty in the Control Room at any given time.

5. *Control Room Administration and Procedures*

5.1 An incident log will be maintained in the Control Room and details of all incidents will be noted together with any action taken.

5.2 It is recognised that images of identifiable living individuals obtained by the System comprise personal data and are subject to the law on data protection including the provisions of the Act. All copies will be handled in accordance with the procedures outlined in Appendix II of this Code, which is designed to ensure the integrity of the System. The Security Manager will be responsible for the development of and compliance with the working procedures in the Control Room.

5.3 Recorded images will only be reviewed with the authority of the Security Manager or nominee. Copies of images are permitted only for the purposes of crime detection, evidence in relation to matters affecting safety, evidence for prosecutions, evidence for disciplinary proceedings in

accordance with clauses 6 and 7 below, for the purpose of car park management or where otherwise required by law.

6. Covert Recording

6.1 Covert cameras may be used only in the following circumstances and only with the written authorisation of, or upon the request of, the Security Manager if:

- informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- there is a reasonable cause to suspect that unauthorised or illegal activity is taking place or is about to take place.

6.2 Any covert recording will only be carried out for a limited and reasonable period of time. It must be consistent with the objective of making the recording and must only relate to the specific unauthorised activity.

6.3 The decision to adopt covert recording will be appropriately documented and will detail how the decision to use covert recording was reached, the length of time it is to continue for and by whom.

7. Workforce Monitoring

7.1 The System may capture images of staff members during its operation. These images will only be viewed or used for workforce monitoring purposes if the University has reasonable suspicion of criminal activity, gross misconduct or behaviour which puts others at risk.

7.2 If images of staff members caught by the System are to be used either in disciplinary proceedings, criminal or civil proceedings then the footage will be retained until after these proceedings have concluded. Retention will be for such period as is necessary according to the purpose(s) for which the images were obtained or have been retained, in accordance with the Records Retention Schedule.

7.3 Staff members have the right to view any images of them which have been captured by the System and also have a right to respond to such images.

7.4 In addition to being informed in this Code, there will also be signs placed at the entrance and at strategic points throughout the University, informing staff that CCTV is in operation.

7.5 No images will be captured from areas in which staff members would have an expectation of privacy, for example the toilets or changing facilities in the University.

8. Staff

8.1 All staff involved in the operation of the System will, by training and access to this Code, be made aware of the sensitivity of handling CCTV images and recordings.

8.2 The Security Manager will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions, operational and administrative, arising from the System.

8.3 All staff using the System will be trained on the University's obligations, and its and their responsibilities, arising from the Act.

8.4 Operatives of the System not directly employed by the University (for example, contract security staff) will be required to hold a valid SIA licence before they are permitted to access the System.

9. Recording & Retaining

9.1 The System and local systems are supported by digital hard drive recording facilities. The digital recording facility is capable of retrieving images to a dedicated server or to an external device.

9.2 Images will be cleared automatically after holding for 28 days unless otherwise required to keep for evidential purposes or a Subject Access Request has been received before the images are due for deletion. However, the University recognises that, in accordance with the requirements of the Act, no images should be retained for longer than is necessary. Accordingly, some recorded images may be erased after a shorter period, for example, where it can be determined more quickly that there has been no incident giving rise to the need to retain the recorded images.

9.3 In the event of the disc or digitally recorded image being required for evidence or the investigation of crime it will be retained for a period of time until it is no longer required for evidential purposes or any investigation into a crime has been completed.

9.4 In order to comply with the standards set out in the ICO's Code of Practice:

- the medium on which images are captured will be cleaned so that images are not recorded on top of images recorded previously;
- the medium on which images have been recorded will not be used again when it has become apparent that the quality of further images has deteriorated; and
- where the system records features of the camera and/or date and time reference, these will be checked for accuracy on a regular basis.

9.5 Where images are to be downloaded, the minimum number of copies necessary to achieve the purpose shall be created. Any such copies shall be destroyed once they are no longer required for the purpose. All such copies shall be recorded onto new CD-R or DVD-R and shall be encrypted. Each disc shall be stored in accordance with annex 2.

9.6 Hard copy prints of digital images are subject to the same controls and principles of data protection as other data collected in the Control Room. They will be treated using the same procedures (contained within Appendix II of this code) as digital images.

10. Monitoring Procedures

10.1 Manning of the Control Room will be by authorised officers only. The officers are members of the University's Security Staff or Contracted Security staff.

10.2 The control of the System will always remain with the University but at the University's discretion the cameras may be operated in accordance with requests made by the police during an incident to:-

- monitor potential public disorder or other major security situations;
- assist in the detection of crime; and
- facilitate the apprehension and prosecution of offenders in relation to crime and public order.

On each occasion that the Police obtain assistance with their operations, a report setting out the time, date and details of the incident must be submitted to the Security Manager.

11. Digital Recording Procedures

11.1 ***Control and management of digital recordings***

All discs belong to and remain the property of the University. Disc handling procedures are in place to ensure the integrity of the image information held (see paragraph 8).

11.2 ***Third party access to recordings***

Generally, requests by persons outside the University for viewing or copying of discs or obtaining digital recordings will be assessed by the Security Manager or nominee on a case-by-case basis. All requests for disclosure will be approached with caution. The University has discretion to refuse any request for disclosure, unless there is an overriding legal obligation.

Access to recorded images will only be granted where it is consistent with the obligations placed on the University by the Act, the University's Data Protection Policy and, in particular, with the purposes set out in paragraph 1.1 of this Code.

12. Standards

12.1 It is important that access to, and disclosure of, the images recorded by the System is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of the System will also have to ensure that the reasons for which they may disclose copies of the images are compatible with the reasons or purposes for which they originally obtained those images. These aspects of the Code reflect the Second and Seventh Data Protection Principles of the Act.

12.2 All Control Room staff will be made aware of the restrictions set out in this Code in relation to access to, and disclosure of, recorded images.

12.3 Access to recorded images will be restricted to staff who need to have access in order to achieve the purposes of using the System.

12.4 All access to the medium on which the images are recorded (disc or digital) will be documented.

12.5 Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances, and only to the extent required or permitted by law:

- law enforcement agencies where the images recorded would assist in a specific criminal inquiry;
- prosecution agencies;
- relevant legal representatives;
- where it is deemed necessary by the Security Manager or nominee to identify a victim, witness or perpetrator in relation to a criminal incident. Images from the system may be circulated via the University e-mail system to selected staff on a targeted basis or placed on a restricted area of the University's website. As part of that decision, the wishes of the victim of an incident will, where possible, be taken into account; and
- where disclosure is required by virtue of the Act.

12.6 When Disclosure to a third party is granted, the University will ensure:

- arrangements are in place to restrict disclosure of images in a way consistent with the purposes set out in paragraph 1.1 of this Code;
- consideration is given to whether images of individuals need to be obscured to prevent unwarranted identification or distress;
- the images are disclosed in a way that is secure to ensure they are only seen by the intended recipient; and
- appropriate records are maintained.

12.7 All requests for access or for disclosure will be recorded. The Security Manager or nominee will make decisions on access to recorded images by persons other than police officers. Requests by the police for access to images will not normally be denied provided that they are accompanied by a written request signed by a police officer, who must indicate that the images are required for the purposes of a specific crime enquiry.

12.8 If access or disclosure is denied by the Security Manager, the reasons will be documented and filed.

If access to or disclosure of the images is allowed then the following will be documented:

- the date and time at which access was allowed and/or the date on which disclosure was made;
- the reason for allowing access or disclosure;
- details of who the images have been provided to (name of the individual and the organisation (where applicable);

- the extent of the information to which access was allowed or which was disclosed;

- the Security Manager or nominee, using the appropriate forms will document routine disclosure to the police

See paragraph 12 for access by data subjects.

13. Access by Data Subjects

13.1 All individuals whose images are recorded have a right to request to view the images of themselves held by the University and, unless they agree otherwise, to be provided with a copy of the images in most circumstances (a **Subject Access Request**).

13.2 All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of a Subject Access Request.

13.3 Data subjects will be provided with a standard Subject Access Request form which requires individuals to provide:

- dates and times when they visited the University and their location, for example which campus site and specific area or building;

- two photographs of themselves - one full face and one side view with the completed form;

- proof of their own identity e.g. a utility bill, a driving licence or a passport;

- either a cheque or cash to the sum of £10.00 for which a receipt will be issued at the time of the issue of the form (statutory payment required in respect of a Subject Access Request); and

- They will be asked whether they are satisfied with merely viewing the images recorded or require a copy of the images.

13.4 A written decision on their request will be sent to them within 20 working days and if access to the images is to be provided (see paragraph 13 below for circumstances when it may be refused), such access will be provided within 40 days of the University receiving the request or, if later, the date when the University receives the identification evidence and the appropriate fee from the data subject. Disclosure will not be made until identification details and the appropriate fee are received by the University

13.5 The University may refuse a request for a copy of the data, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. If it is decided that a Subject Access Request be refused, the reasons will be fully documented and the data subject informed of the reasons in writing within 20 working days.

13.6 Copies of Subject Access Request forms must be sent to the University's Data Protection Officer for audit and record-keeping purposes.

14. *Rights of Data Subjects*

14.1 The procedure outlined above and the use of the Subject Access Request form complies with Section 7 of the Act, enabling the Security Manager or nominee to inform individuals as to whether or not images have been processed by the System. The University is not obliged to comply with a request under this section unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the information which that person seeks.

14.2 Where the University cannot comply with the request without disclosing information relating to another individual who can be identified from that information, it is not obliged to comply with the request unless:

- the other individual has consented to the disclosure of the information to the person making the request; or

- it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

14.3 Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to the Security Manager, who will provide a written response within 20 working days of receiving the request, setting out their decision. A copy of the request and response will be retained.

Appendix I

Nominated Staff who may view live stream CCTV

Name	Position
Gill Firth	School Manager – Computing and Engineering
Sarah Wickham	Archivist and Records Manager
Laurie Nettleton	Sports Manager
	Library Wardens
Jane Mcparland	Student Union Shop Manager
Heather Mackintosh	Executive Office Manager – Vice-Chancellor's Office
David Bray	Team Leader – Computing and Engineering
Dennis Town	Technical Services Manager – Computing & Engineering
Michael Fish	Lecturer – Human & Health Sciences

Nominated Staff who may also record and playback CCTV

Name	Position
Vince Deer	Library Support Officer
Wayne Winterbottom	IT Support Manager
Paula Clover	Customer Services Manager

APPENDIX II

Code of Practice for the Operation of CCTV

PROCEDURES FOR THE HANDLING OF CCTV IMAGES

Computer disks-Still photographs

All computer disks containing CCTV images, or any still photograph or printed image, shall be marked with a unique number. A log will be maintained by the Security Manager or nominee containing details as to the dates when the disk/photograph was introduced into the system or created and when it was disposed of. Computer disks, still photographs and hard copy prints will be disposed of as confidential waste. Such erasure and disposal will be logged

Disclosure of images to third parties

In this section "Authorised Data Handler" means, the Security Manager or nominee.

The Police

Where a police officer requests access to CCTV images (hereafter referred to as Data), either by viewing such Data, or requesting a copy of such Data, then an Authorised Data Handler shall complete, sign and date Part A of the appropriate Data Protection form (copy contained within Appendix III) containing details of the Data required.

The police officer shall complete, sign and date Part B, which contains the reasons for requiring the data; his/her name rank and number, police station address, crime/incident number if applicable and property reference number.

When the form has been completed, the Authorised Data Handler may pass the required data to the police officer requiring it.

The completed form shall be handed to the Security Manager or nominee to be retained for evidential purposes.

Other person

The Security Manager or nominee, having been satisfied as to the bona-fide of the person requesting access to Data and that the reasons for so requesting access, fall within the exemptions contained within sections 28(1), 29(1)(a) and (b) and 35(2)(a) of the Act, may authorise such access, by signing and dating

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

Part B of the appropriate Data Protection form (copy contained with Appendix IV). On receiving such authorisation an Authorised Data Handler shall complete, sign and date Part A of the form containing details of the data required.

The person requiring access shall complete, sign and date Part C of the form, which contains the reasons for requiring the data, his/her name, home/business /agency name and address (whichever is applicable) together with any applicable reference number.

When the form has been completed and it is deemed that disclosure should be made the Authorised Data Handler may pass the required Data to the person requiring access.

Other persons may include law enforcement agencies (other than the police), Solicitors, Private individuals.

(An example of a private individual being given access to the data would be where a victim of a theft, is permitted to view a recorded image to point out to an investigator the exact location where an item subject to theft was located. This would allow the investigator to view the images and concentrate their attention on that location).

The Security Manager or nominee shall retain the completed form for evidential purposes.

APPENDIX III

DATA PROTECTION ACT 1998

Disclosure of data to the Police

Section A University representative making disclosure/handing over copy

Department……

Reference No ……

Name……..

Signature…… Date…….

Section B Reason Data required (To be completed by Police Officer)

I am making enquiries concerned with the investigation of a crime. This application is made in accordance with the provisions of the Data Protection Act 1998, Sections 28(1), 29(1)(a), 29(1)(b) and/or 35(2)(a) and, as such, it is confirmed that the personal data is required for:

Nature of enquiry:

The information sought is needed to:

I can confirm that the personal data requested is for the purpose(s) stated above and failure to disclose the data would, in my view, be likely to prejudice that/those purpose(s).

Signature……Date……..……..

Name…….Rank.....……

Police Force……Station……...…….

Countersigned……Rank……..……..

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

(This application must be authorised by a person who is senior to the requesting officer, and of a rank no lower than Inspector)

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

APPENDIX IV

DATA PROTECTION ACT 1998

Disclosure of Data to Persons other than the Police

Section A. University representative making disclosure/handing over copy

Department……

Reference: ……

Name……..

Signature…… Date…….

Section B Authorisation for disclosure by Security Manager/nominee

Name…….

Position……..

Signature……... Date……..…

Section C Reason Data required (To be completed by person requesting data)

I can confirm that the above data is required by me for any of the following reasons contained within sections 28(1), 29(1)(a) and (b) and 35(2)(a) of the Act.

(Please tick as required)

- For the purpose of safeguarding national security ☐
- The prevention or detection of crime or the apprehension or prosecution of offenders ☐

- For the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings) ☐
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights ☐

Name…….
Position *(if applicable)*……..
Business/Agency *(if applicable)*……..…
Business/Agency/Home address (*whichever is applicable)*……..…

Signature……Date……

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019

Reference No……

Version:	23/05/2016
Policy Owner(s)	Estates and Facilities
Policy Approved by	Estates and Facilities
Date of Approval	May 2016
Date for review	May 2019