POLICY

POLICY INSTRUCTION

CLOSED CIRCUIT TELEVISION SYSTEM (CCTV)
CODE OF PRACTICE & OPERATING PROCEDURES

CCTV CODE OF PRACTICE

1. DEFINITIONS

For the purposes of this Code of Practice, the following definitions will apply:

- **'University'**
  University of Wolverhampton

- **'Scheme/system'**
  The University's closed circuit television scheme.

- **'Body Worn Recording Devices (Images and Sound)'**
  Body worn recorded devices do not fall within the classification of CCTV, however, the University will manage all data from body worn recorded devices in line with this code of practice as appropriate. These can be live streamed to the Control Room and can be activated from the Control Room in the event of an emergency. Any BC that has been activated from the Control Room should be recorded on IRAMS and authorised by the Security Manager or his nominee

- **'Control Room/Campuses'**
  City Campus, Walsall Campus, Science Park, Springfield, ESMS, Telford Campus and all Control Rooms are covered by the contents of this policy and procedures.

2. SCOPE

This Code of Practice is binding on all employees and students of the University of Wolverhampton, all employees of contracted out services and apply to all other persons who may, from time to time, and for whatever purpose, be present on University premises.

3. OWNERSHIP AND OPERATION OF THE SCHEME

- The University of Wolverhampton owns the closed circuit television scheme, which operates at the University.

- All recorded material is owned by, and the copyright of any material is vested in, the University.

- The Security Service, whose personnel are employed directly by the University, operates the scheme.

4. PRINCIPLES

The following principles will govern the operation of the scheme:

- The scheme will be operated fairly and lawfully and only for the purposes identified by the University of Wolverhampton.
- The scheme will be operated with due regard for the privacy of the individuals.
- Any change to the purposes for which the scheme is operated will require the prior approval of University of Wolverhampton in advance.
- To ensure the security and integrity of the Security Service operating procedures, these will be implemented and amended only with the prior consent of the Security Manager

5. PURPOSE OF THE SCHEME

The purposes of the scheme are as follows:

- To assist in safeguarding the personal security and health and safety of students of the University; employees of the University, visitors to the University and members of the public passing through University campus and utilising University car parking facilities.
- To assist in safeguarding property belonging to students of the University; employees of the University, visitors to the University and members of the public passing through University campus and utilising University car parking facilities.
- Provide improved security of University property.
- To aid the prevention, deterrence and detection of crime and in this regard to provide evidence for internal disciplinary hearings, the police and other bodies with prosecuting powers such as HM Customs and Excise and the Health and Safety Executive.

6. KEY OBJECTIVES

The key objectives of the scheme are as follows:

- To prevent, detect and reduce the incidence of crime, in particular theft of property belonging to individuals and to the University.
- To detect, prevent and reduce offences against the person.
- To detect, prevent and reduce any instances of criminal activity related to drugs and other illegal substances.
- To reduce instances of vandalism and other criminal damage.

CCTV CODE OF PRACTICE (CONT'D)

6. KEY OBJECTIVES (CONT'D)

- To prevent and enable the University to respond effectively to any harassment and bullying.

- To improve the efficiency with which the University is able to alert the police to any unlawful activity.

7. DATA PROTECTION ACT 1998

- The University's scheme will be registered for the purposes of the Act. The Data Protection Principles established by the Act will, where appropriate; be used by the University as a guide in the operation of the scheme:

  - Recorded material shall be obtained and be processed fairly, lawfully and in accordance with this Code of Practice.

  - Recorded material shall be held lawfully and only for the purposes of this Code of Practice.

  - Recorded material shall not be used or disclosed for any purpose, or in any manner, which is incompatible with this Code of Practice.

  - Recorded material shall be adequate, relevant and not excessive in relation to the purposes set out in this Code of Practice.

  - Where recorded material is retained for any of the purposes set out in this Code of Practice, that material shall not be kept for longer than is necessary for the purpose for which it is being retained and shall be stored in a secure manner requiring authorised access.

  - Access to recorded material will be permitted strictly in accordance with this Code of Practice and the operating procedures detailed for the Security Section.

- The University will ensure that appropriate security measures are taken to prevent unauthorised access to, the alteration of, disclosure or destruction of any recorded material; and to prevent accidental loss or destruction of such material.

- Recorded material will not be sold, used for commercial purposes, used for the provision of entertainment or used to provide information or material for research purposes.

CCTV CODE OF PRACTICE (CONT'D)

8. USE OF RECORDED MATERIAL AND STILL IMAGES

- Where video image is used to identify a particular individual, that individual will be allowed to apply for access to a recording subject to the protection of the interests of other individuals who are on the recording, in accordance with the Freedom of Information Act 2000. Requests can be made via the Information and Records Manager.

- Still photographs will be generated from recordings made by the system only where these are required for evidential purposes by the police or other bodies with prosecuting powers, or by the University. No copies shall be made.

- Unless required to do so by a court of law, recordings made by the system and/or still images generated from such recordings will not normally be made available by the University to individuals wishing to use them as evidence in any civil litigation.

- The University of Wolverhampton reserves the right to use a recording made by the system and/or still images generated from such recordings, in any civil prosecution brought by the University.

- The University of Wolverhampton reserves the right to use a recording made by the system and/or still images generated from such recordings, as evidence in internal grievance/complaints investigations and/or in disciplinary investigations involving students or employees of the University.

9. TARGETED OBSERVATION

- Where necessary, and in compliance with the declared purposes and key objectives of the scheme and the protocols governing the provision of evidence, the system may be used for targeted observation.

- No sound monitoring facility is provided with the cameras.

10. RESPONSIBILITIES OF THE OWNER OF THE SCHEME

It is the responsibility of the University, as the owner of the scheme:

- To ensure compliance with the Code of Practice.

- To approve and ensure compliance with the operating procedures for the scheme.

- To notify persons entering areas monitored by the scheme that a closed circuit television system is in operation.

- To provide copies of this Code of Practice when requested to do so.

CCTV CODE OF PRACTICE (CONT'D)

11. MANAGEMENT OF THE SCHEME

- The Security Manager manages the scheme on a day-to-day basis.
- The Director of Estates and Facilities Directorate, as the nominee of the Vice-Chancellor, is the person of the University designated as having overall responsibility for security matters.
- Access to the University's system, to the University Security Control Room and access to/release of recordings made by the system, will be strictly in accordance with the operating procedures established by University Security Management

12. INSTALLATION

- Any installation connected with the scheme will be appropriate to its purposes and to the requirements of this Code of Practice.
- When installing cameras that may overlook any residential accommodation, the University will have regard for the privacy of any residents.

13. MONITORING AND EVALUATION

This Code of Practice, its operation and the operation of the University's system will be reviewed annually by the Security Manager or a nominated person

14. BREACHES OF THE CODE OF PRACTICE

The University reserves the right to take disciplinary action against any employee or student who breaches this Code of Practice.

15. HEALTH AND SAFETY

A purpose of the University's scheme is that it should be used to assist in safeguarding the health and safety of students, employees, visitors and members of the public. It should be noted that any intentional or reckless interference with any part of the scheme (including cameras) may constitute a criminal offence and will be regarded as a breach of discipline.

16. COMPLAINTS PROCEDURE

Grievances and complaints concerning the operation of the University's closed circuit television system may speak to the Security Manager, Campus Operations Facilities, City Campus or a nominated representative. If complaints remain unresolved this can be escalated through the universities complaints procedure

17. GENERAL ENQUIRER

Enquiry's concerning this Code of Practice and/or the operation of the scheme should be directed to the Security Manager, University of Wolverhampton, City Campus

DATA HANDLING PROCEDURES

18. Images captured by the system will be monitored in the Control Room at each location and centrally at City Campus. The Control Room is self-contained and secure room and the monitors cannot be seen from outside its room.

19. No unauthorised access to the Control Room is allowed at any time. Normal access is strictly limited to the Duty Controllers, authorised staff members, Police officers may enter with the explicit consent of the Security Manager or his nominee. A list of University staff authorised for routine access to the Control Room will be compiled and maintained.

20. Persons other than those specified in paragraph 19 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 his/her nominee. Each separate visit will require individual authorisation and will be supervised, at all times, by the (Security Manager) or his/her nominee. Such visitors will not be given access to any data, which falls within the scope of the Act.

21. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may be granted to persons with a legitimate reason to enter the Control Room.

22. Before granting access to the Control Room, Controllers 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 details of 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 Controllers on duty in the Control Room at any given time.

CONTROL ROOM ADMINISTRATION AND PROCEDURES

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

24. It is recognised that the images obtained comprise personal data and are subject to the law on Data Protection. All copies will be handled in accordance with the procedures outlined in appendix I of this Code, and are 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.

25. Recorded images will only be reviewed with the authority of the Security Manager or his/her nominee. Copies of recorded or digital images will only be made for the purposes of the scheme paragraph 5.

STAFF

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

27. The (Security Manager) will ensure that all staff, including relief staff, are fully briefed and trained in respect of all functions, both operational and administrative, arising within the CCTV control operation. Training in the requirements of the Data Protection Act and this Code of Practice will also be provided.

RECORDING

28. The Control Room system is a digital recording system, which is capable of retrieving images to a digital system.

29. Images are recorded digitally; the process of identifying retrieval dates and times is computerised. Images will be cleared automatically after a set time.

30. Unless required for evidential purposes or the investigation of crime, recorded images will be retained for no longer than 31 days from the date of recording. However, the University recognises that, in accordance with the requirements of the Data Protection 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.

31. In the event of the 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.

MONITORING PROCEDURES

32. Controllers, who will be members of the University's Security Staff, will be available to work in the Control Rooms throughout the twenty-four hour day.

33. 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;
- Facilitate the apprehension and prosecution of offenders in relation to crime and public order.

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

DIGITAL RECORDING PROCEDURES

34. **CONTROL AND MANAGEMENT OF DIGITAL RECORDINGS**

All discs belong to and remain the property of University of Wolverhampton. Disc handling procedures are in place to ensure the integrity of the image information held (see paragraph 30).

DIGITAL RECORDING PROCEDURES (CONT'D)

35. ACCESS TO RECORDINGS

Generally, requests by persons outside the University for viewing or copying of or obtaining digital recordings will be assessed on a case by case basis.

Requests from the Police will arise in a number of ways, including: -

- Requests for a review of recordings, in order to trace incidents that have been reported.
- Immediate action relating to live incidents e.g. immediate pursuit.
- For major incidents that occur, when images may have been recorded continuously.
- Individual Police Officer seeking to review recorded images within the Control Room.

Access by data subjects will be in accordance with paragraph 42 below.

Requests for access to recorded images from persons other than the Police or the data subject will be considered on a case-by-case basis. The (Security Manager) or his/her nominee will consider such requests. Access to recorded images in these circumstances will only be granted where that is consistent with the obligations placed on the University by the Data Protection Act 1998.

36. STANDARDS

It is important that access to, and disclosure of, the images recorded by CCTV 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 CCTV 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 Data Protection Act 1998.

37. All control room staff should be aware of the restrictions set out in this Code of Practice in relation to access to, and disclosure of, recorded images.

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

39. All access to the medium on which the images are recorded, will be documented.

40. Disclosure of the recorded images to third parties will be made only in the following limited and prescribed circumstances, and 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.

DIGITAL RECORDING PROCEDURES (CONT'D)

41. (CONT'D)

- Where it is decided by the (Security Manager) or his/her nominee that the assistance of the
  University staff is needed 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.

- People whose images have been recorded and retained and disclosure is required by virtue of the Data Protection Act 1998.

All requests for access or for disclosure will be recorded. The (Security Manager) or his/her 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 and can be made without the above authority provided 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.

If access or disclosure is denied by the (SECURITY MANAGER), the reasons will be documented and forwarded to the Control Room for filing.

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 or the date on which disclosure was made.

- The reason for allowing access or disclosure.

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

- Control Room staff using the appropriate forms will document routine disclosure to the Police.

- Requests for non-Police disclosures will be forwarded to the (Security Manager).

- See paragraph 9 for Access by Data Subjects.

ACCESS BY DATA SUBJECTS

42. All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of subject access requests via the Information and Records manager.

CODE OF PRACTICE ON THE OPERATION OF CCTV

APPENDIX I

PROCEDURES FOR THE HANDLING OF CCTV IMAGES

COMPUTER DISKS-STILL PHOTOGRAPHS/PRINTED IMAGES

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 within the Security Department and managed by the Security Coordinator this will contain details as to the dates when the disk/photograph/print was introduced into the system or created and when it was disposed of. An entry will be made in the log of any dates the disk/photograph/print was removed from the control room, together with the identity of the person removing it and the reason for such removal.

DISCLOSURE OF IMAGES TO THIRD PARTIES

In this section "Authorised data handler" means, the Security Manager or his/her nominee and any University Security Officer.

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, then an authorised data handler shall complete, sign and date Part A of the appropriate Data Protection form (copy contained within Appendix II) 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 PERSONS

The (Security Manager) or his/her nominee, having been satisfied as to the bona-fide of the person requesting access to CCTV images (hereafter referred to as data) and that the reasons for so requesting access, fall within the exemptions contained within sections 28(1), 29(1)(a) an (b) and 35(2)(a) of the Act, may authorise such access, by signing and dating Part B of the appropriate Data Protection form (copy contained with Appendix III). 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 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 his/her nominee shall retain the completed form for evidential purposes.

CODE OF PRACTICE ON THE OPERATION OF CCTV

APPENDIX II

DATA PROTECTION ACT 1998

DISCLOSURE OF DATA TO POLICE

Section A Description of Data required to be disclosed (To be completed by University representative)

DISCS:

VIEW: ☐ TAKE POSSESSION OF ☐ (TICK AS REQUIRED)

Camera Name(s) .....

Times and dates of Recordings .....

.....

DATA CONTAINED WITHIN DOCUMENTS

VIEW: ☐	TAKE POSSESSION OF:ORIGINAL ☐	COPY ☐	GIVEN VERBALLY: ☐ (TICK AS REQUIRED)

Description of document(s)

.....

.....

DISCLOSURE OF DATA CONTAINED WITHIN COMPUTERISED RECORDS

State what data is required and where data stored

.....

.....

.....

.....

October 2018

UNIVERSITY REPRESENTATIVE MAKING DISCLOSURE.

Department……

Name……..

Signature…… Date…….

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

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.

(tick as required)

- For the purpose of safeguarding national security ☐
- The prevention or detection of crime ☐
- 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……Collar Number……

Police Force……Station……..

By accepting this data I understand that I become responsible for the correct handling procedure in accordance with the data protection act 1998 and in accordance with the recommendations of the Information Commissioners Office.

Signature……Date……..

Other than Found Property Number for articles taken into session……..

Crime/Incident No……

October 2018

APPENDIX III
DATA PROTECTION ACT 1998

DISCLOSURE OF DATA TO PERSONS OTHER THAN THE POLICE

Section A:

Description of Data required to be disclosed (To be completed by University representative)

Disc:

VIEW: ☐	TAKE POSSESSION OF ☐	(TICK AS REQUIRED)

Camera Name(s) .....

Times and dates of Recordings .....

.....

Data contained within documents

View: ☐	Take possession of: Original ☐	Copy ☐	Given verbally: ☐	(Tick as required)

Description of document(s)

.....

.....

.....

Disclosure of Data contained within computerised records.

View: ☐	Take possession of: Disc copy: ☐	Printout ☐	Given verbally: ☐

State what data is required and where data stored (i.e. home address of named person; occupant of named address etc-From E-Vision)

.....

.....

.....

October 2018

UNIVERSITY REPRESENTATIVE MAKING DISCLOSURE.

Department……

Name……

Signature……

Date……..

SECTION B. AUTHORISATION FOR DISCLOSURE BY SECURITY MANAGER/NOMINEE

Name……

Signature……

Position……

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.

(tick as required)

- For the purpose of safeguarding national security ☐
- The prevention or detection of crime ☐
- 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 ☐
- For the purpose of an internal investigation by the University of Wolverhampton ☐

Name……

Position (If applicable)……

Business/Agency (if applicable)……

Business/Agency/Home address (Whichever applicable)……

……

By accepting this data I understand that I become responsible for the correct handling procedure in accordance with the data protection act 1998 and in accordance with the recommendations of the Information Commissioners Office.

Signature……Date……

Reference No……

October 2018