



The Open  
University

The Open University  
Closed Circuit Television Code of Practice



The Open  
University

Issue	Prepared By	Date	Checked & Approved By	Date
Draft	Steve Molloy	May 2009		
Draft 2	Steve Molloy	July 2009		
Draft 3	Peter Ling	July 2009		
Draft 4	Peter Ling	Sep 2009		
Draft 5	Peter Ling / Shoosmiths	Nov 2009		
Draft 6	Peter Ling (DP/Shoo/AFW)	Aug 2010		
Draft 7	Peter Ling	Sep 2010		
Issue 1	Peter Ling	Feb 2011	Mary Legge	Feb 2011
Issue 2	Stephen stone	Feb 2012	Mary Legge	Feb 2012
Issue 3	Steve Molloy	Feb 2013	Mary Legge	Feb 2013

**Approved for Distribution**

By:

Date: 21/02/13

If not signed above, then document is for reference purposes only, not for distribution and not subject to amendment control.



The Open  
University

## Definition of Terms

CCTV – Closed circuit television

Security Team – Part of the Operations Group within Estates, based at Walton Hall

University – The Open University, its staff and its Estate

SOP – Standard Operating Procedure

The Commissioner's Code - Government Document CCTV Code of Practice prepared by the Information Commissioner

## 1. Introduction

This code of practice is based upon the principles set out in the Government Document CCTV Code of Practice prepared by the Information Commissioner (the Commissioner's Code) and is compliant with the Human Rights Act 1998 and the Data Protection Act 1998.

The fundamental objective of the University CCTV system is to make University premises safer environments in which to work, learn and carry out recreational pursuits.

The CCTV installation on University property is entirely owned by the University and operated by the Security Team. Additional cameras not on University property, owned by others, but linked to the University system are operated by the Security Team.

The operation of the University CCTV system complies with the National Occupational Standards for CCTV Operations.

## 2. Purpose

### 2.1 Key Objectives

The purpose and Key objectives of the University's CCTV System is;

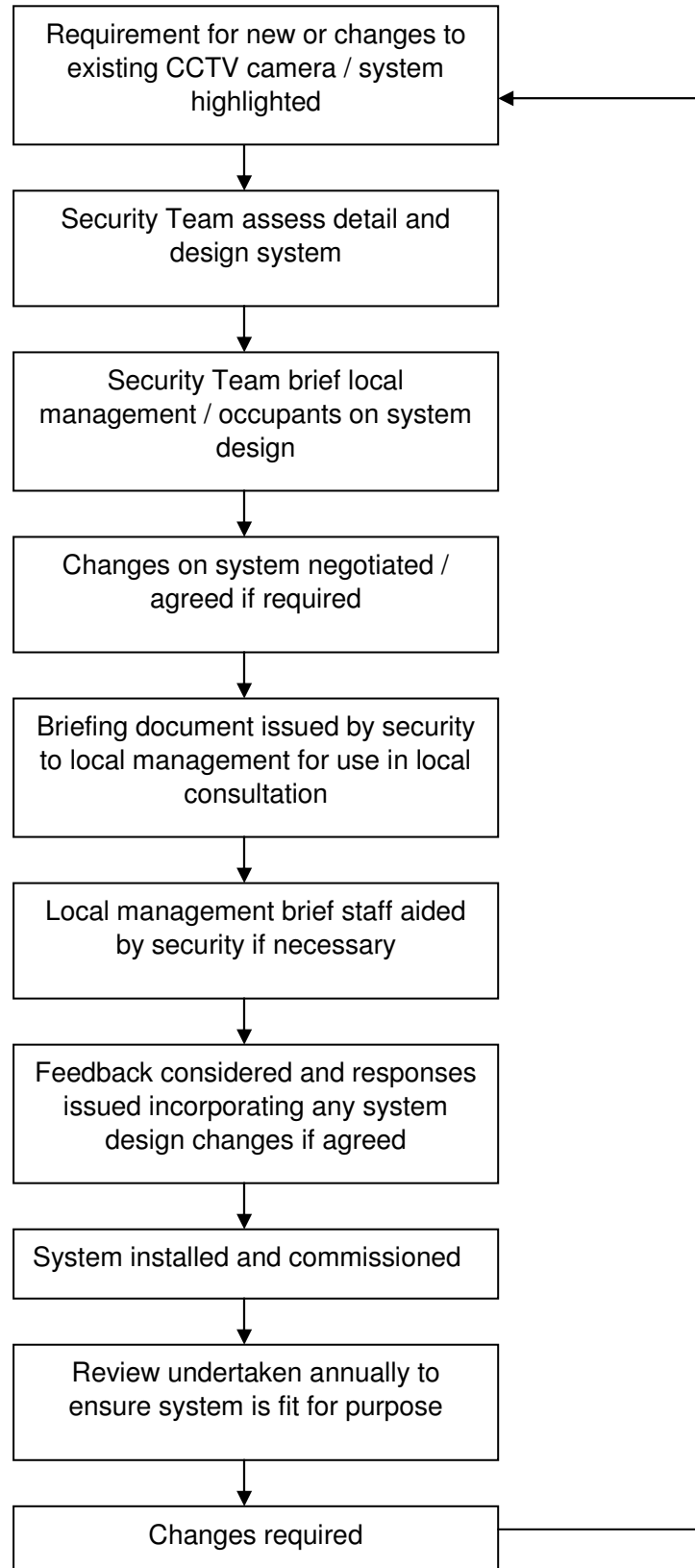
- To provide a safer environment by the prevention and detection of crime
- To prevent the escalation of anti-social incidents and minimise their harmful impact.
- To provide quality evidence to aid the identification, apprehension and prosecution of offenders.
- To provide a deterrent against crime and anti-social incidents
- To help improve the management and safety of traffic and pedestrian movements
- To provide a more efficient use of University Security resources to deal with crime and anti-social incidents.
- To help alleviate the fear of crime and enhance community safety.



The Open  
University

## **2.2 Installation and Design**

When a requirement for an extension to the CCTV System is highlighted the process below will be followed to ensure the views of stakeholders are considered.





The Open  
University

## **3. Privacy and Data Protection**

### **3.1 Public Concern**

The majority of the public has become accustomed to being observed by CCTV systems in towns and cities and accepts that such systems may be in the public interest when properly managed. The Open University recognises that those who do raise concerns do so mainly over matters pertaining to the processing of the data recorded i.e. what happens to the material that is obtained. A crucial thread throughout this Code of Practice is that the University is responsible and accountable for the data.

In processing personal information there must be respect for the privacy of the individual. With this in mind the Commissioner's Code must be followed in both spirit and to the letter.

### **3.2 Data Protection Act.**

The Open University CCTV system is installed and will be used in a way that complies with the Data Protection Act 1998. The day to day operation of the system is the responsibility of the Duty Warden, overseen by the Security Manager.

All data will be processed in accordance with the eight principles of the Data Protection Act .

## **4. Accountability and Public Information**

### **4.1 Access to CCTV Facilities.**

For reasons of security and confidentiality, access to the Security Control room is restricted in accordance with this Code of Practice. However in the interest of openness and accountability, anyone wishing to visit the room may be permitted to do so, subject to the approval of, and after making prior arrangements with, the Security Manager or an approved Deputy.

The University operates a formal complaints procedure. Complaints should be made to the Security Manager. Any complaint made in relation to any aspect of the University's CCTV system will be recorded and investigated. Complaints will be dealt with in accordance with existing grievance and disciplinary procedures which apply to all members of staff of the Open University, including the CCTV operators. Any contract staff will be dealt with under their company's procedures and the terms of the contract with the Open University.

### **4.2 Signage**

Nationally recognised signs will be placed at entrances to sites and in the locality of cameras advertising the presence and operation of CCTV cameras. Information on the signs shall be sufficient to ensure that University staff and visitors will be in no doubt that CCTV cameras are in operation and will include contact details of the Security Team.



The Open  
University

## **5. Human Resources**

### **5.1 CCTV Monitoring within the Security Control Room.**

The CCTV Monitoring will be staffed in accordance with SOP's. Only authorised personnel who have been properly trained in its use and all monitoring room procedures will operate equipment associated with the Open University CCTV System.

These staff will have been recruited following standard third party/University recruiting procedures and undergone additional screening in accordance with the Security Industry Authority and/or British Standards.

Arrangements may be made for the Police to be present in the monitoring room at certain times, subject to locally agreed protocols or the Regulation of Investigatory Powers Act 2000. Any such person must be conversant with these Codes of Practice and associated Procedural Manual.

### **5.2 Locally Monitored Systems**

Where parts of the Open University CCTV System cannot, for technical reasons, be connected directly to the Security Control Room for that part of the systems data to be recorded, local recording equipment will be installed at each of these locations. (e.g. certain regional sites) The Open University CCTV system undertakes all recording in digital format. All data will be managed in accordance with the principles of this Code of Practice.

Recording and retrieval of such systems will be undertaken only by trained staff while monitoring will be undertaken by staff trained and authorised to manage these local facilities.

The Open University may locate CCTV monitors showing real time views of the local system/camera coverage which, although designed for staff usage may be observed by the general public. This openness of information is not regarded as a breach of confidentiality as it will only show brief moments of the cameras' view of public areas where an expectation of privacy will not be reasonably held.

### **5.3 Non-monitored Systems/Mobile CCTV Units**

Only authorised personnel who have been properly trained will handle the mobile non-monitored system.

### **5.4 Discipline**

All personnel involved with the system shall receive the appropriate training in respect of legislation relevant to their role.

Any unauthorised use of the Open University CCTV System for any purpose whatsoever will be judged to be gross misconduct according to the University's Disciplinary Procedures.



The Open  
University

## 6. Management of Recorded Material

For the purpose of this code “recorded material” means any material recorded by, or as a result of, technical equipment which forms part of the Open University’s CCTV System, but specifically includes images recorded digitally, or on video tape or by way of video copying, including video prints.

All CCTV recording equipments used in conjunction with the Open University’s CCTV System may contain material that will at a later date be required to provide evidence at a criminal court or disciplinary hearing. Continuity of evidence, as directed in the SOPs, is to be maintained to ensure best evidence is produced to satisfy the rule of law/disciplinary procedures. The chain of evidence handling must be maintained to the highest degree to ensure the integrity of the evidence. Members of the community must have total confidence that the information recorded about their ordinary, every day activities by virtue of the system, will be treated with due regard to the right of respect for the individual.

It is therefore important that all images, of whatever format (e.g. paper copy, video, CD or DVD) obtained from the system are treated in accordance with this Code of Practice, procedural manual and SOP from the moment they are received by the monitoring room until final destruction.

Access to, and the use of, recorded material will be strictly for the purposes defined in this Code of Practice only.

Each recorded incident will have a unique reference number automatically assigned to it for reference. Recorded incidents can further be protected or archived in order to maintain the integrity of the recorded image. Non protected/Archived images will be automatically overwritten after a maximum of 90 days.

Recorded material will not be copied, sold, otherwise released or used for commercial purposes or for the provision of entertainment.





The Open  
University

## **7. Access to Recorded Material**

An individual whose personal data is held by the University in the form of a CCTV recording can request access to that recording. The University will respond in accordance with the Data Protection Act 1998. All requests for the release of recorded information should be referred to the University's Data Protection Office.

The University may release recorded CCTV material and prints of such material to the Police or other authorised agency for the purposes of the prevention or detection of crime, the apprehension or prosecution of offenders, or in other circumstances where the University is legally obliged to do so, or in accordance with the specified purposes of the CCTV system. This will be done on the authority of the Security Manager or his Deputy.

The identity of the individuals on the CCTV recording but not relevant to the investigation or the request for access will be obscured unless the individuals have given their consent. The identity of the individuals on the recording whose presence is relevant to the investigation or request for access will be disclosed if they give consent to this, and may be disclosed if this consent is refused when deemed reasonable to do so in the circumstances.

No other access will be allowed unless approved personally by the Security Manager or his Deputy and only then for reasons which fall within the purposes and objectives of the University's security policy and in accordance with this Code.

## **8. Release of Recorded Material**

Where the Police are investigating an alleged offence, they may release details of recorded information to the media only in an effort to identify alleged offenders. Under those circumstances full details must be recorded.

If material is shown to potential witnesses, including police officers, for the purpose of obtaining identification evidence, it must be shown in accordance with the Commissioner's Code.

Any request from the media for recorded CCTV material of a particular occurrence, (usually in respect of criminal proceedings) must be referred to the Security Manager or his Deputy.

## **9. Evaluation**

The CCTV Policy will periodically be evaluated to establish whether the purposes of the scheme are being met and whether objectives are being achieved.

The evaluation will include:

- An assessment on the impact on crime at University locations.
- A comparative assessment of crime in areas without CCTV.
- Continuing relevance and location of equipment.
- Operation of the code.



## **The Data Protection and Human Rights Acts**

### **1 The Data Protection Act**

The Data Protection Act 1998 requires that all processing of personal data including CCTV systems and video recordings conform to the eight principles of the Act. In compliance with these principles, the Open University will only record data for the purposes as indicated in this Code of Practice. Section 163 of the Criminal Justice and Public Order Act 1994 empowers the University to provide apparatus/equipment for the recording of visual images of events/incidents occurring on its property if it considers this will promote the prevention of crime or welfare of the victims of crime.

The eight principles of the Data Protection Act are;

1. All personal data must be obtained and processed fairly and lawfully. For the purpose of this principle, adequate signage has been strategically placed at numerous locations upon the University premises, informing the public that that CCTV surveillance is in operation upon its premises.
2. Personal data must be processed only for the purposes specified. To comply with this principle, recordings are only used for the purposes and disclosed only to the people described in this code of practice.
3. Personal data held must be adequate, relevant and not excessive in relation to the purpose for which the data are held. Therefore installation and changes to systems follow the consultation process shown in point 2.2 of this code.
4. Personal data must be accurate and where necessary kept up to date. To comply with this principle, the University maintains the system so that it is fit for the purposes described in this code.
5. Personal data must be held for no longer than is necessary. Generally recordings are kept for a minimum of 31 days and not longer than the period it takes for the system to overwrite the recordings, 90 days, or as long as it may be required for criminal investigations and proceedings.
6. Personal data must be processed in accordance with the rights of data subjects. Individuals are allowed to access information held about them and, where appropriate, request its correction or erasure.
7. Information must be secure. Security measures are in place to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information. These will be enhanced as necessary.
8. Personal information must not be transferred to countries without adequate protection. Should the University need to transfer any recordings outside the UK, adequacy checks will be made on the destination organisation or country.



The Open  
University

## 2 The Human Rights Act

The Human Rights Act 1998 became law on 2 October 2000, which incorporated the rights and liberties enshrined in the European Convention of Human Rights (the Convention), which guarantees a range of political and freedoms of the individual against interference by “public authority”. Article 8 of the Convention refers to rights of privacy of an individual. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in the interests of the national security, public safety, economic well being of the country, prevention of disorder or crime, protection of health and morals and protection of the rights and freedom of others. The Human Rights Act has an impact on the use of CCTV, as the processing of such data and images may affect the rights of an individual. Wherever CCTV is used to record images of individuals, clear and legible signage should be in positions so that the public are aware of the CCTV surveillance.