



The  
University  
Of  
Sheffield.

Estates & Facilities  
Management



**The University of Sheffield**

**Closed Circuit Television**

**Code of Practice**

## Contents

<b>Section</b>	<b>Page</b>
<b>Introduction</b>	<b>1</b>
<b>Use of CCTV and Complaints</b>	<b>2</b>
<b>1. Why CCTV is used – Aims and Objectives</b>	<b>2</b>
<b>2. The System</b>	<b>4</b>
<b>3. Maintenance of the System</b>	<b>5</b>
<b>4. The Control Room</b>	<b>5</b>
4.1 Stand Alone Systems	6
4.2 Body Worn Cameras	6
<b>5. Control Room Administration and Procedures</b>	<b>6</b>
5.1 Staff	6
5.2 Liaison	7
5.3 Recording	7
5.4 Camera Control	7
<b>6. Digital Recording Procedures</b>	<b>8</b>
6.1 Access to Recordings	8
6.2 Standards	8
6.3 Access by Data Subjects	10
6.4 Rights of Data Subjects	10
6.5 Digital Images	11
6.6 Disposal	11
<b>Appendices</b>	
A Application Form – Access to Information	12

## Introduction

The University of Sheffield has installed a comprehensive CCTV surveillance system. Cameras have been installed throughout the main campus and the residences incorporating the main traffic routes both in and around the University. Some of the cameras are fully operational with pan, tilt and zoom (PTZ) facilities, which are monitored both at a central control room on the main campus and at the residences monitoring room. Others are fixed cameras, images of which are presented in the two same rooms. Staff are also issued with body worn cameras used by security staff when on late night patrols and dealing with drunkenness, violence and anti-social behaviour. Six call-point cameras are installed at key locations. These are linked direct to the control room/ monitoring room to allow students, staff and members of the public who feel vulnerable or threatened to contact a qualified member of security staff. This service will operate 24hrs a day. Secondary monitoring and recording facilities are located as stand-alone systems in other areas and are operated on site.

This Code of Practice has been prepared for the guidance of managers and the operators of the CCTV system and for the information of all members of the University community. Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the University, consistent with the obligations on the University imposed by the General Data Protection Regulation (GDPR) (and associated regulations) and DPA CCTV code of practice revised editions 2008 and 2013

The Information Commissioner's Office (ICO) issued its first code of practice under the Data Protection Act 1998 (DPA) covering the use of CCTV. In 2000 the code was developed to explain the legal requirements operators of surveillance cameras were required to meet under the Act and promote best practice. The code also addressed the inconsistent standards adopted across different sectors at that time and the growing public concern caused by the increasing use of CCTV and other types of surveillance cameras.

The unwarranted use of CCTV and other forms of surveillance cameras has led to a strengthening of the regulatory landscape through the passing of the Protection of Freedoms Act (POFA). The POFA has seen the introduction of a new surveillance camera code issued by the Secretary of State since June 2013 and the appointment of a Surveillance Camera Commissioner to promote the code and review its operation and impact. The ICO has contributed to this tougher regulatory landscape by taking enforcement action to restrict the unwarranted and excessive use of increasingly powerful and affordable surveillance technologies. At this time, Universities are not currently classed as "relevant authorities", however Sheffield University CCTV system will voluntarily comply with the terms of the Code of Practice issued under the POFA to further emphasise the safe and proper use of CCTV at Sheffield University.

## Use of CCTC and Complaints

The CCTV systems at Sheffield will be used with utmost probity and in accordance with operational standards, complying with current legislation. However, it is recognised that members of the University and others, whose images are captured on the system may have concerns and questions about the use of CCTV. In the first instance, any query should be directed to the Head of Security Services (Ext 29232). The system is registered with the Information Commissioner and can only be used in accordance with those registered aims and objectives. These are contained in this Code of Practice.

The University's Data Protection Officer can also be contacted regarding any concerns (Ext 21117)

### 1. Why CCTV is used – Aims and Objectives

CCTV has been installed to reduce the fear of crime generally and to provide a safe public environment for the benefit of those who live, work or visit the University or its environment consistent with respect for individuals' privacy.

These objectives will be achieved by the monitoring of the system, to:

- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public disorder; and as an aid to public safety.
- Provide the Police, Health and Safety Executive and University with evidence upon which to take criminal, civil and disciplinary action respectively.
- To assist in the University's Emergency procedures.
- To assist in Civil Emergencies.
- To assist with traffic management.
- To promote safer communities.
- Provide a Training facility.
- Provide and operate the system in a manner, which is consistent with respect for the individual's privacy.

The legal basis for processing under the General Data Processing Regulation are the following Articles:

6(1)d: vital interests of the data subject

6(1)e: processing carried out in the public interest

6c(1)f: the legitimate interests of the Data Controller

### Procedural and administrative notes

The Head of Security Services of the University retains overall responsibility for the system and delegates the day to day management to the Security Operations Manager and his/her Deputy. It is their responsibility to ensure that CCTV within the University is managed in line with this Code of Practice, the current CCTV Code of Practice produced by the Information Commissioner's Office and the current Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner.

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

The objectives outlined in paragraph 1 of this code will be closely followed when assessing the requirements for new CCTV installations. Similarly, if designated usage of the area changes it will be necessary to assess whether the location of cameras remains justified in meeting the stated purpose and whether there is a case for removal or relocation.

### Responsibilities

It is the responsibility of the Head of Security Services or in their absence the Security Operations Manager and his/her Deputy to:

- Have in place a system whereby cameras are only sighted in locations that show a pressing need for surveillance in accordance with the aims and objectives.
- Ensure the CCTV system complies with the GDPR and associated legislation
- Manage the process of image and data retention, security and viewing by authorised persons
- Regularly evaluate the system to ensure it complies with the latest legislation, Codes of Practice and offers the best value to the University of Sheffield.



## 2. The System

The system consists of:

- Overt PTZ and static cameras – local, residences and campus area. Controlled from 3 dedicated terminals, 2 in the University Emergency control room and 1 in the residences monitoring room.
- Images recorded at 7 frames per second. Live viewing at 25 frames per second.
- Help Points – local and campus area. Two- way sound and image recorded with speak facility.
- Synetics integrated system on dedicated fibres, interfaces and operating software – Central Control Room and Residences Monitoring Room.
- Static cameras – Central Campus, Residences and Hospitals
- Body Worn Cameras – used by security staff when on late night patrols and dealing with drunkenness, violence and anti-social behaviour

Given that CCTV cameras cover a wide area of the University Campus and areas to which members of the public has access, every effort will be made to inform the students, staff and public by way of signs at regular intervals and at the entrance zone of areas covered by cameras.

Signs will be placed at the entrance to the CCTV zone to inform the public of the presence of the system and its ownership.

Clear and prominent signs are particularly important where the cameras themselves are discreet, or are in locations where people might not expect to be under surveillance.

Images captured on camera will be transmitted either to a central control room, Residences Monitoring station or to separate stand-alone systems where they will be recorded for use in accordance with this Code of Practice. Although every effort has been made in the planning and design of the CCTV 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.

For the purposes of the GDPR, the Data Controller is the University of Sheffield and the University is legally responsible for the management and maintenance of the CCTV system.

### **3. Maintenance of the System**

To comply with the GDPR (Articles 5, 24, 25 and 32), the CCTV systems will be maintained in an efficient and effective manner, ensuring images comply with the quality standards expected under the legislation. A maintenance agreement is in place setting out the terms of how the system will be maintained and improved.

Emergency attendance by engineers is part of the maintenance agreement and any faults will be rectified without delay. This is to ensure a service is provided to the students, staff and public within the CCTV area.

### **4. The Central Control Room & Residences Monitoring Station**

Members of the public are not allowed to have access to control rooms or monitoring areas.

Images captured by the system will be monitored in the Central Control room and Residences Monitoring Station, both self-contained and secure rooms. The monitors cannot be seen from outside of the rooms.

No unauthorised access to the control room or monitoring station will be allowed at any time. Normal access to it will be strictly limited to the duty controllers, authorised staff members and senior management. Police officers may enter with the consent of the Security manager or his nominee.

Staff and visitors may be authorised to enter the control room or monitoring station on a case-by-case basis. Authorisation is required and may only be given by the Security manager or Operations manager. Each separate visit will require individual authorisation. In an emergency and where it is not reasonably practicable to secure prior authorisation, access may also be granted to persons with a legitimate reason to enter the control room.

Before granting access to the control room or monitoring station, staff must satisfy themselves of the identity of any visitor and 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 and of any visitors to the control room in an emergency.

#### **4.1 Stand Alone Systems**

Stand-alone monitoring and recording systems located at porters lodges and Faculties, will also comply with all aspects of the CCTV Code of Practice. Assistance in the management of each individual system is available by contacting the Head of Security Services on Ext 29232.

#### **4.2 Body Worn Cameras**

BWC are used by security staff when on foot patrol and images are required to provide evidence of offences or other behaviour that might require action by security. Persons subject to recording by BWV will be made aware that it is in use by the security officer making a verbal announcement unless circumstances prevent that from happening.

Recording will only take place when there is a valid reason for doing so. Images that are recorded will be managed in accordance with this Code of Practice and the GDPR (Articles 6(1)d, 6(1)e and 6(1)f).

### **5. Control Room / Monitoring Room Administration and Procedures**

An incident log will be maintained in the Central Control room/ Monitoring Room and kept securely there. Full details of incidents will be noted in it together with any consequential action taken.

Control room operations require the use of a number of confidential written records and logs. These will be established on an “as required” basis and will be outlined in the Operations Manual but not accessible to the public generally..

#### **5.1 Staff**

All staff are trained in current legislation as it applies to CCTV taking into account:-

- The General Data Protection Regulation and associated legislation
- The Human Rights Act 1998
- The Protection of Freedoms Act 2012
- The Freedom of Information Act 2000
- The Regulation of Investigatory Powers Act 2000

In addition, all staff are trained in the effective operation of CCTV equipment and processes in order to comply with Code of Practice and current legislation. CCTV operators do not currently fall into the category that requires a licence from the Security Industry Authority.

## 5.2 Liaison

CCTV forms part of the larger picture in respect of community safety and in particular the Sheffield Safer Communities. The Head of Security Services will act as liaison officer on behalf of the University and receive feedback from other agencies in the furtherance of good CCTV practice. This will also act a public liaison as required by the Surveillance Camera Commissioners Code of Practice.

## 5.3 Recording

The control room system is supported by digital recording facilities, which will function throughout operations at 7 frames per second. In addition incidents can be recorded in 'real time' where necessary at 25 frames per second. Digital images will be automatically erased after a set period, which will be no longer than 7 days with the exception of cameras in licensed commercial premises which will be held for a period of 31 days.

In the event of digitally recorded image being required for evidence, they will be retained for a period recommended by the police.

Images may also be retained in excess of the 7 day period when they are required for non-crime or civil litigation or other lawful reason, for example, a health and safety incident requiring a protracted investigation.

## 5.4 Camera Control

Staffing of CCTV control rooms and monitoring rooms will be in accordance with the operations manual. Control rooms require a 24hr response and will be staffed sufficiently to provide this service.

Whilst the CCTV system always remains under the control of the University, when a request is received from agencies with a law enforcement role for assistance, any such assistance will only be given in accordance with the law and after due consideration by the Head of Security Services who will reserve the right to refuse assistance if it is deemed unlawful or not appropriate to the aims and objectives of the scheme.

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 Head of Security Services. Details of such incidents will be recorded on the Incident reporting information system log (IRIS)

## 6. Digital Recording Procedures

All discs belong to and remain the property of the University of Sheffield. Recording handling procedures are in place to ensure the integrity of the image information held (see Section 6.3).

## 6.1 Access to Recordings

If the request is made by Police, access will be given for valid lawful reasons and in accordance with the Operations Manual procedure.

Generally, access will; be requested for investigation of offences, fast time actions, e.g. pursuits. Post event investigation to trace witnesses or obtain evidence.

If access is requested by a third party, for example an Insurance Company, the request will be considered under the GDPR Articles 6(1)c, 6(1)e and 6(1)f and the Human Rights Act 1998 in order to protect the privacy of persons recorded. Requests for data under the GDPR Article 15 (Subject Access) are dealt with by a clear process set out in the operations manual and accompanied by a subject access request form. Members of the public are entitled to apply for a copy of data under this process.

Data will only be released if it is for one of the aims and objectives of the scheme.

## 6.2 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 to third parties are compatible with the reasons or purposes for which they originally obtained those images, in accordance with Data Protection legislation. (The reasons for obtaining and recording images via CCTV are set out in paragraph 1.1 of this Code under *Objectives*).

All control room staff are aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

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

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

Disclosure of the recorded images to third parties or to other individuals or departments within the University will be made only in the following limited and prescribed circumstances:

- Law enforcement agencies where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies.
- Authorised relevant legal representatives.
- Where it is decided after full consultation by the University's senior management team and South Yorkshire Police that the public's assistance is needed to identify a victim, witness or perpetrator in relation to a criminal incident, images from the system will be provided to the media. 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 GDPR Article 15.

All requests for access or for disclosure will be recorded. Decisions on access to recorded images by persons other than police officers will be made by the Head of Security Services, if required the final decision will be made by the University Data Protection Officer. Requests from the Police will not normally be refused but will require a formal request, signed by an officer using the requisite form.

If the Head of Security Services or Data Protection Officer denies access or disclosure, the reasons will be documented and forwarded to the Control Centre for filing.

If access to or disclosure of the images is allowed by the Head of Security Services in non-police cases or by a member of the control room staff where the proper format has been followed - as above - in police cases, 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. \*
- Routine disclosure to the police will be documented by control room staff using the appropriate forms, which will be filed with a copy of the authorising officer's written request (see above).
- Requests for non-police disclosures will be forwarded to the Security Manager. \*

\*See also below, at 6.3 'Access by Data Subjects'.

### **6.3 Access by data subjects**

All staff involved in monitoring or handling image data will proceed in accordance with the following protocol in respect of subject access requests. Data subjects will be provided with a standard subject access request form which:

- Requires individuals to provide dates and times when they visited University and their location - for example which campus site and specific area or building.
- The individuals will provide two photographs of themselves - one fullface one side view with the completed form.
- They will provide to the person receiving the application proof of their own identity e.g. a utility bill, a driving licence or a passport.
- They will be asked whether they would be satisfied with merely viewing the images recorded.
- A written decision on their request will be sent to them within one month of receiving a valid request.

### **6.4 Rights of Data Subjects**

The procedure outlined above and the use of the data subject form complies with Article 15 of the GDPR, enabling the Data Protection Officer or their nominee to inform individuals as to whether or not images have been processed by the CCTV 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.

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.

Information setting out the detail in paragraph 6.4 will be provided with the subject access form.

In the case of a request under Subject Access rules, where the images form part of a criminal investigation and to release them would interfere with that investigation, the University may decline their release.

## 6.5 Digital Images

Digital images taken from digital recorders are subject to the same controls and the same principles of data protection as other data collected in the control room. They may only be obtained to assist the identification, apprehension and prosecution of alleged offenders, during staff training and for other purposes consistent with the purposes of the CCTV system set out in paragraph 1 above. Control room staff using equipment available in the control room may only produce photographic material.

Digital images will normally be supplied to the police upon reasonable request. Any requests for viewing a digital image other than a police request will be considered by the security manager in liaison with the Data Protection Officer.

All Digital images produced must be recorded along with the identity of the requesting person, date and other appropriate information in the **transfer of data log**.

## 6.6 Disposal

Recordings will be destroyed after 7 days unless required for evidential purposes, in accordance with Article 5(e) of the GDPR.

**Richard Yates Head of Security Services Security Services**

**APPX A**

### **How to Apply For Access To Information Held On the CCTV System**

These notes explain how you can find out what information, if any, is held about you on the CCTV System.

### **Your Rights**

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort, or if you agree otherwise. The University of Sheffield will only give that information if it is satisfied as to your identity. If release of the information will disclose information relating to another individual(s), who can be identified from that information, the University is not obliged to comply with an access request unless

- The other individual has consented to the disclosure of information, or
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual(s)

#### **The University's Rights**

The University of Sheffield may deny access to information where the legislation allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- Prevention and detection of crime
- Apprehension and prosecution of offenders

And giving you the information may be likely to prejudice any of these purposes.

October 201

**THE APPLICATION FORM: (N.B. ALL sections of the form must be completed. Failure to do so may delay your application.)**

**Section 1** Asks you to give information about yourself that will help the University to confirm your identity. The University has a duty to ensure that information it holds is secure and it must be satisfied that you are who you say you are.

**Section 2** Asks you to provide evidence of your identity by producing TWO official documents (which between them clearly show your name, date of birth and current address) together with a recent full-face and side view photograph of you.

**Section 3** Asks you to confirm whether you will accept just viewing the information, or if you want a copy of the information.

**Section 4      You must sign the declaration**

When you have completed and checked this form, take or send it together with the required TWO identification documents and photograph to:

**Data Protection Officer, The University of Sheffield, Edgar Allen House, 241  
Glossop Road, Sheffield S10 2GW**

If you have any queries regarding this form, or your application, please ring the CCTV System Manager on 0114 2229232

**SECTION 1 About Yourself**

**The information requested below is to help the University (a) satisfy itself as to your identity and (b) find any data held about you.**

**PLEASE USE BLOCK LETTERS**

<b>Title (tick as appropriate)</b>	<b>Mr</b>	<input type="checkbox"/>	<b>Mrs</b>	<input type="checkbox"/>	<b>Miss</b>	<input type="checkbox"/>	<b>Ms</b>	<input type="checkbox"/>
<b>Other title (Dr., Rev., etc.)</b>	<input type="text"/>							
<b>Surname/family name</b>	<input type="text"/>							
<b>First names</b>	<input type="text"/>							
<b>Maiden name/former names</b>	<input type="text"/>							
<b>Sex (tick box)</b>	<b>Male</b>	<input type="checkbox"/>	<b>Female</b>	<input type="checkbox"/>				
<b>Height</b>	<input type="text"/>							
<b>Date of Birth</b>	<input type="text"/>							
<b>Place of Birth</b>	<b>Town</b> <input type="text"/>							
	<b>Country</b> <input type="text"/>							
<b>Your Current Home Address (to which we will reply)</b>	<input type="text"/>							
	<input type="text"/>							
	<input type="text"/>							
	<b>PostCode</b> <input type="text"/>							
<b>A telephone number will be helpful in case you need to be contacted.</b>	<b>Tel. No.</b> <input type="text"/>							

*If you have lived at the above address for less than 10 years, please give your previous addresses for the period:*

**SECTION 4 To Help us find the Information**

December 2016 Version: 07

<i>Previous address(es)</i>		
<i>Dates of occupancy</i>	<i>From:</i>	<i>To:</i>
<i>Dates of occupancy</i>	<i>From:</i>	<i>To:</i>

**SECTION 2 Proof of Identity**

**To help establish your identity your application must be accompanied by TWO official documents that between them clearly show your name, date of birth and current address.**

**For example: a birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address.**

**Also a recent, full-face photograph of yourself.**

**Failure to provide this proof of identity may delay your application.**

**SECTION 3 Supply of Information**

**You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to?**

**a) View the information and receive a permanent copy**

**b) Only view the information**

**SECTION 4 Declaration**

**DECLARATION (to be signed by the applicant)**

**The information that I have supplied in this application is correct and I am the person to whom it relates.**

**Signed by**

**Date**

**Date**

**Warning – a person who impersonates or attempts to impersonate another may be guilty of an offence.**

**NOW – please complete Section 4 and then check the 'CHECK' box (on page 5) before returning the form.**

***If the information you have requested refers to a specific offence or incident, please complete this Section.***

***Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet, in the same way, if necessary.***

***If the information you require relates to a vehicle, property, or other type of information, please complete the relevant section overleaf.***

**Were you: (tick box below)**

<b><i>A person reporting an offence or incident</i></b>	<input type="checkbox"/>
<b><i>A witness to an offence or incident</i></b>	<input type="checkbox"/>
<b><i>A victim of an offence</i></b>	<input type="checkbox"/>
<b><i>A person accused or convicted of an offence</i></b>	<input type="checkbox"/>

<b><i>Other – please explain</i></b>	
<b><i>Date(s) and time(s) of incident</i></b>	
<b><i>Place incident happened</i></b> <b><i>Brief details of incident</i></b>	

*Before returning this form  
Please check:*

- ***have you completed ALL Sections in this form?***
- ***Have you enclosed TWO identification documents?***
- ***Have you signed and dated the form?***

***Further Information:***

***These notes are only a guide. The law is set out in the General Data Protection Regulation, obtainable from The Stationery Office. Further information and advice may be obtained from:***

The Data Protection Officer The University of Sheffield Edgar Allen House 241 Glossop Road Sheffield, S10 2GW	The Office of the Information Commissioner Wycliffe House Water Lane Wilmslow Cheshire, SK9 5AF
tel: 0114 222 1117	tel: 01625 545 745

***Please note that this application for access to information must be made direct to The University of Sheffield (address on Page 1) and NOT to the Data Protection Commissioner.***

**OFFICIAL USE ONLY**

*Please complete ALL of this Section (refer to 'CHECK' box above).*

**Application checked and leaible?**  **Date Application Received**

**Identification documents checked?**

**Details of 2 Documents (see page 3)**

<input type="text"/>	<input type="text"/>

**Documents Returned?**

*Member of Staff completing this Section:*

<b>Name</b>	<input type="text"/>	<b>Location</b>	<input type="text"/>
<b>Signature</b>	<input type="text"/>	<b>Date</b>	<input type="text"/>

