Surveillance Camera

Code of Practice

(Version 15)

Contents

Introduction

The University of Sheffield has a comprehensive surveillance camera system which has been in place since 1998. This system has grown and developed over time and as at March 2025, has over 1200 cameras. Cameras are installed throughout the main campus, the residences and the Innovation Campus, 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, others are fixed cameras. All are centrally monitored in a central control room on the main academic campus with a secondary fallback facility based at the residential campus and a fallback facility. UoS Campus Safety and Security (CS&S) staff are also issued with body worn cameras which are carried at all times whilst on duty. Six call-point cameras are installed at key locations. These are linked directly to the control room/ fallback 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 operates 24 hrs a day.

The University has made effective use of improvements in technology over time. In 2025, UoS changed its surveillance camera operating platform to AVADA. All surveillance cameras continue to be monitored centrally and are now digitally recorded into UK based cloud servers managed by AVADA.

This Code of Practice has been prepared for the guidance of managers and the operators of the surveillance camera system and for the information of all members of the University community. Its purpose is to ensure that the surveillance camera 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), the Data Protection Act 2018, the Information Commissioner's guidance as it relates to the Biometrics and Surveillance Camera Commissioner's (BSCC) Surveillance Camera Code of practice (as amended in November 2021)

At this time, Universities are not currently classed as "relevant authorities", however the University of Sheffield have voluntarily accepted those responsibilities.

Aims and Objectives

The surveillance camera system 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
- 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

Surveillance cameras will not be used to generally monitor staff activity and performance. The University will only use surveillance cameras in staff disciplinary proceedings where there is a suspicion of misconduct. In these situations the investigating manager or HR Manager / Advisor will formally request access to images from the Data Protection Team (see Access to Digital Images), 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 this code will be closely followed when assessing the requirements for new surveillance camera 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.

Ownership and operation of the scheme

The Surveillance camera scheme is owned and operated solely by the University of Sheffield and the University is legally responsible for the management and maintenance of the surveillance camera system. The University will have in place effective processes and resources to ensure the continued maintenance and upgrading of the system.

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

Any change to the Aims and Objectives of the scheme will require the **prior** approval of the Chair of the UoS Executive Board Health and Safety Committee.

For the purposes of the GDPR, the Data Controller is the University of Sheffield. UoS has contract arrangements for system maintenance and some hosting services. These contractors are agreed by the UoS Data protection officer as Data processors.

The surveillance camera system and its operatives are not required to be licensed under the Security Industry Authority scheme.

Management Responsibilities

The Head of CS&S retains overall responsibility for the system and delegates the day to day management to the CS&S Management team. It is their responsibility to ensure that surveillance cameras within the University are managed in line with this Code of Practice.

It is the responsibility of the Head of CS&S and CS&S Management team 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.
- 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.
- Approve the operating procedures for the scheme and to ensure that these operating procedures have been complied with
- Ensure that the Aims and objectives of the scheme are not exceeded.
- Approve any temporary 'Stand Alone' surveillance camera systems as required
- Notify persons entering the University that a Surveillance camera system is in operation using appropriate signage
- Review and update this Code of Practice and the associated Data Protection Impact Assessment[1] annually.
- Provide access to this Code of Practice when requested to do so.
- Provide an annual report relating to the operation and performance of the surveillance camera system.

[1] DPIA in conjunction with the Data Protection Officer

System Description

The system consists of:

- Overt PTZ, 360, panoramic and static cameras – local, residences and campus area. Controlled remotely from the security control room or by local users with relevant access.
- Help Points – local and campus area. Two- way sound and image recorded with speak facility.
- AVADA integrated system on dedicated fibres, interfaces and operating software – Central Control Room and Fallback facility.
- Static cameras – Central Campus, Residences, Innovation Campus.
- Body Worn Cameras – Used by UoS Security staff in accordance with the Campus Safety and Security Operational Standards.
- Ability to monitor the system using internet based web browsing with Individual dual verification log on and audit security.

Given that surveillance cameras cover a wide area of the University Campus and areas to which members of the public have 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 surveillance camera 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.

Although every effort has been made in the planning and design of the surveillance camera 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.

Maintenance of the System

The surveillance camera system 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 surveillance camera area.

The Central Control Room & Fallback facility

Images captured by the system will be monitored by trained operatives, surveillance camera contractors or data protection officers through the secure platform. The platform is able to be accessed remotely through client enabled devices where appropriate. Access is managed on a case by case basis through the CS&S team with support from Data Protection.

Staffing of surveillance camera control rooms will be in accordance with the CS&S Operational Standards. Control rooms require a 24hr response and will be staffed sufficiently to provide this service. All controllers are trained in current legislation and policy as it applies to surveillance cameras 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
- Investigatory Powers Act 2016
- This Code of practice

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

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 (including approved contractor staff) and senior management. Police officers may enter with the consent of the CS&S Management Team where access to view the system is required. Members of the public are not allowed to have access to control rooms or monitoring areas.

Staff and visitors may be authorised to enter the control room or fallback on a case-by-case basis where authority has been given to view images. Authorisation is required and may only be given by the CS&S Management team. Each separate visit will require individual authorisation.

Before granting access to the control room or fallback, staff must satisfy themselves of the identity of any visitor and that the visitor has the appropriate authorisation and recorded as appropriate.

Stand Alone Systems

At the current time there are no Stand alone systems authorised for use in or around University premises. If any such schemes are in place they are not authorised and will be considered as being in breach of this Code of Practice.

From time to time, there may be a need to approve temporary additions to surveillance camera provision which may not be able to be centrally monitored and recorded. Where this is the case, these schemes MUST be submitted in writing to the Head of CS&S, who will ensure that such schemes are operating in accordance with this code of practice and are in line with the Aims and Objectives of the scheme.

Body Worn Video Cameras

The use of Body Worn Video Cameras (BWVC) has been approved by the University. BWVC are used across the University, mainly but not exclusively by CS&S staff and Campus Wardens. BWVC are used to improve the safety of staff, students, and visitors of the University. Evidence indicates that the use of BWVC may reduce the incidence of aggression and violence whilst also providing greater transparency and enabling increased scrutiny for any subsequent actions taken in response to such occurrences. Recording will only take place when there is a valid reason for doing so.

Individuals are likely to have a strong expectation of privacy in places not generally open to the public, such as their private residence, especially at a time of day when occupants are likely to be in bed. Clear justification of the necessity to use BWVC will be required in such circumstances. BWVC should not be used in private spaces, such as toilets, changing rooms, student personal accommodation unless there is a compelling need directly related to the physical safety of staff or others.

All staff must be suitably trained and accredited by the CS&S Operations Manager prior to carriage and use of BWVC. UoS CS&S staff do not currently fall in a category requiring licensing by the Security Industry Authority. BWVC operation is in accordance with this code and specific instructions for staff are available in the Campus Safety and Security Operational Standards.

Persons subject to recording by BWVC will be made aware that it is in use by the security officer making a verbal announcement unless circumstances prevent that from happening.

Targeted Observations

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 observations by trained controllers. Where there is cause to conduct targeted observations, these should be logged on the incident management system (ISARR).

Police or other law enforcement agency requests for targeted observations must be approved by the CS&S Management team and be authorised by law enforcement agencies under the provisions of the Investigatory Powers Act 2016. An ISARR record will be created and will include the authorisation reference number. Where urgency provisions apply, authority may be granted but a record of an authorising police inspector will be recorded.

Community & Agency Liaison

Surveillance camera systems form part of the larger picture in respect of community safety and in particular the Sheffield Safer Communities. The Head of CS&S will act as liaison officer on behalf of the University and receive feedback from other agencies in the furtherance of Surveillance camera system good practice. This will also act as a public liaison as required by the Biometrics and Surveillance Camera Commissioners Code of Practice.

Data Protection Privacy Impact Assessment

Users of surveillance camera systems must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified. Surveillance camera systems require careful consideration in regard to expectations of privacy and the management and security of the data that is held.

Good practice, including Principle 2 of the BSCC Code of Practice requires that a Data Protection Impact Assessment (DPIA) is undertaken whenever the development or review of a Surveillance system is considered. A DPIA also helps assure compliance with obligations as data controller under the data protection legislation.

The UoS of Sheffield has a DPIA in place which will be reviewed when any changes are made and/ or annually.

Recording of Digital Images.

The control room system is supported by digital recording facilities, which will function throughout operations at Images recorded at 12 or 24 frames per second and 1080p where available. All images are digitally recorded UK based cloud servers including person by person security audit.

All Digital images captured by the UoS Surveillance camera system are recorded cloud based servers owned and managed by AVADA and located in the UK. Images recorded cannot be digitally altered in any way.

Access to Digital Images

It is important that access to, and disclosure of, the images recorded by Surveillance cameras 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. Access to recorded images will generally be restricted to staff who need to have access in order to achieve the Aims and Objectives of the system. 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.

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:

- For UoS Disciplinary, training or Health and Safety purposes.
- Law enforcement agencies where the images recorded would assist in a specific criminal inquiry.
- Prosecution agencies.
- Authorised relevant legal representatives.
- Subject access request under GDPR Article 15.

Any requests for access to Surveillance camera images from Third parties or wider UoS staff will be made in writing and approved by the Data Protection team.

Where images may be required for the purposes above these images are securely shared, via the data protection team, with the relevant party. In the event of an emergency, this can also be done by approved control room staff / contractors under the direction of the Security Management team. Where a copy is retained, this will have a unique reference number and the number and the grounds for retention will be recorded on the ISARR incident management system. Access is provided by the data protection team using secure data transfer with dual verification.

Access can be provided by the CS&S Management team for the Police or other Law Enforcement agencies where there is an urgent need. This access will be in accordance with the Incident procedures, recorded and notified to the Data team.

Access by direct live viewing of Surveillance images will be managed and audited by the Campus Safety and Security management team. This includes both live viewing in the control room and any requests for access to live viewing at other locations. Where this is allowed the access will be via personal secure login and all viewing is audited.

Subject Access Requests

Requests for Subject access under Article 15 GDPR are managed by the UoS Data Protection team. using the procedure detailed in the link below:

UoS Subject access Requests.

Any member of the University's staff or employee of a company or of the security contractor who receives a personal subject access request must forward it immediately to the Data Protection Team.

Data/image retention.

Digital images will be automatically erased after 14 days.

Images retained in licensed commercial premises will be held for a period of 31 days.

Images retained for the purposes of civil, criminal or UoS disciplinary evidence, training, and/or access transfer to data subjects or third parties will be retained for up to 7 years.

Images transferred to the Cloud based transfer system (AVADA) will be retained for up to 7 years.

Breaches of this Code of Practice

The University reserves the right to take disciplinary action against any employee or student who breaches this Code of Practice in accordance with the University's disciplinary procedures.

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

Complaints Procedure

The Surveillance camera system at Sheffield is 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 Surveillance cameras. In the first instance, any query should be directed to the Head of CS&S (security@sheffield.ac.uk).

Complaints specifically relating to the use of Surveillance camera data can be directed to the UoS Data Protection Officer (dataprotection@sheffield.ac.uk).

Complaints by staff and students concerning the operation of the University's Surveillance camera system should also be directed to the Head of Security, but may be progressed through the relevant University grievance/complaints procedures;

Staff grievance procedure. Student Complaints procedure

General Enquiries.

Enquiries concerning this Code of Practice and/or the operation of the University's scheme should be directed to the UoS Head of CS&S (security@sheffield.ac.uk)

This Code of Practice is published on-line on the link below:

UoS Surveillance Camera Code of Practice

Copies can be made available on request.