Code of Practice

for

University of Bath Students' Union Event Control

Revision	Date	Author
1.0	03/01/2016	N Bartley

Appendices

1 System Overview and Management

1.1 Introduction

The Code of Practice aims to introduce measures to ensure accountability, high standards, good quality information and use of the System at University of Bath Students' Union Events covered by the Event Control Room.

All sections of the Code of Practice and operating manual are subject to continuous review and reference should be made to the issue date shown on the front of the document.
The CCTV system will only be used to achieve the aims and objectives as set out in the Code of Practice. Cameras will at no time, without authority, be used to look into private residences / premises. All CCTV users will be trained in accordance with the requirements of the Code of Practice and procedural manuals.

If users are required to hold a CCTV Licence under the terms of the Private Security Industry Act 2003, then they shall not operate the system until they are in possession of such a licence. It is deemed that University of Bath Students' Union Events are private ticketed events and that a Public Space CCTV License is not required.

All users will be aware that any misuse of the system may result in disciplinary proceedings (ie breach of Data Protection Act 1998) and in turn may bring the system into disrepute. The Event Control Room Duty Technician will ensure procedures prevent any misuse of the system from taking place and the necessary records are kept.

No sound recording will be used on the system.

1.2 Location

This Code of Practice relates to the Closed Circuit Television System (CCTV) and related Event Control support systems temporarily installed for University of Bath Students' Union events.

The CCTV and Event Control equipment is not publicly accessible.

1.3 Why is CCTV Installed

Events hosted by University of Bath Students' Union require adequate supervision and coordination by multiple organisations; event security, medical support, event management and technical management.

The CCTV and event control systems allow for centralised monitoring of events attended by large numbers of students, for criminal, medical and major incidents and activity. It also allows for overall coordination of the multiple organisations in response to these incidents.

CCTV is a proven deterrent to the perpetrators of criminal activities and its presence also acts to alleviate the fear of crime in the mind of the law abiding public.
CCTV surveillance is being utilised to deter anti social behaviour and criminal activity.

1.4 Objectives

The scheme aims to:-

- Coordinate personnel in the event of a medical incident
- Coordinate personnel in the event of a security incident
- Coordinate personnel in the event of a major incident
- Assist in the detection and prevention of crime
- To deter those having criminal intent
- To reduce the fear of crime and give confidence to the attendees that they are in a secure environment
- To monitor the flow of attendees throughout the site and monitor for possible overcrowding issues

1.5 Management

The beneficiary of the system is:- University of Bath Students' Union (Bath SU).

The main contact person is:- Mike Dalton

The Data Controller is:- University of Bath Students' Union (Bath SU).

1.6 The Users

There may be more than one user involved in the operating the system. All users must be fully trained and conversant with the requirements of this Code of Practice.

1.7 Partners

All partners to this scheme will sign up to these codes and accept responsibility under the Data Protection Act accordingly.

1.8 Registration

The system is not specifically registered with the Information Commissioner under the Data Protection Act 1988, as it installed on a temporary basis on behalf of University of Bath Students' Union (Bath SU), which is registered.

1.9 Signage

In accordance with the Data Protection Act, signage is in place informing the Public that they are entering an area covered by surveillance equipment. The University of Bath already has signage in place for the area included by this system. Additional signage will be added if deemed necessary.

2 The System

2.1 Introduction

The Event Control Room provides a key hub for the supervision and management of Bath Students' Union Large Events.

The Event Control Room provides a key hub for the transit of radio messages, and the coordination of teams responding to incidents. The Event Control Room also logs messages and incidents where required.

The system provides CCTV surveillance of University of Bath Students' Union Large Events, encompassing entrance queues, perimeter fences, bars, main stage auditoriums and other area where large crowds are likely to gather. Images from the cameras are transmitted to the Event Control Room, where the monitoring, control and recording of the cameras is undertaken.

The system also provides IP telephony services, and internet access to key event areas and the control room.

The system provides act timing and information services for any video display screens as required.

2.2 CCTV Coverage

The level of coverage in the areas with the cameras is designed to cover the main image sizes appropriate to the individual camera use as set out in the operational requirements.

Cameras comprise ptz and fixed static cameras, with some infra-red capability.

2.3 Recording

All the cameras are recorded at the network video recorder located in the Event Control Room. The camera images are recorded digitally. Should copies of images be required for evidential purposes, these will be reviewed in accordance with the release of images to third parties section below.
Management of this access and recording procedure is described in more details in later sections of this Code of Practice. (Section 4.3.12)
The system records images and they will be stored for a period of up to 30 days unless required for evidential purposes, where they will be retained in a secure manner for the Police or other agency. The Event control system is also used to store written information about incidents, observations and information via radio traffic.

2.4 Control of cameras and Personal Data (see Appendix B)

The CCTV cameras from the system can only be monitored, controlled, and recorded by authorised personnel in the Event Control Room. No third party control or access will be allowed without suitable permission.

It is deemed that University of Bath Students' Union Events are private ticketed events and that a Public Space CCTV License is not required under the Private Security Industry Act 2001.

3 Legislative Framework

3.1 Background

University of Bath Students' Union Event Control recognise that the use of CCTV could potentially impact on a member of the public's right to respect for private and family life afforded by Article 8 of the European convention on Human Rights and the Human Rights Act 1998. CCTV will therefore only be used for the purposes set out in section 2 above and no other use will be made of images collected by the system. Where CCTV for covert or targeted surveillance purposes is carried out in accordance with the Regulations of Investigatory Powers Act 2000 (RIPA) it will be subject to the appropriate authority levels.

CCTV systems will be run in accordance with the requirements of the Data Protection Act 1998, Human Rights Act 1998 and requirements laid down in the Information Commissioner's Code of Practice, issued under the Data protection Act 1998. (refer www.ico.gov.uk)

3.2 Human Rights Act 1998

This code will observe Articles 3, 6, 8, 10, 11 and 14 of the Human Rights Act 1998 and will incorporate those safeguards necessary to protect the rights of privacy, except where the law permits specific surveillance activities. (for Human Rights Act 1998 see Appendix A)

3.3 Data Protection Act 1998

All Closed Circuit Television (CCTV) schemes that receive, hold or process personal data are obliged to conform to the Data Protection Act 1998. (for Data Protection Act 1998 information see Appendix B)

The Act covers CCTV systems used in areas where the public would have a "right to visit". These include, but are not limited to:-

- A place that is in private ownership, but where the public perceive no boundary
- A place where a public service is offered
- Public footpaths, roads, bridleways, etc

3.4 Regulations of Investigatory Powers Act 2000 (RIPA)

When it is necessary to carry out 'DIRECTED OR INTRUSIVE SURVEILLANCE' the appropriate authority will be obtained from the relevant authority, see Appendix C of this Code of Practice.

3.5 Subject Access (Access by Data Subjects)

This is a right which is provided by Section 7 of the 1998 Data Protection Act. A detailed explanation and standards are outlined in the Commissioner's Code of Practice.

Applications by Subjects (members of the public) for copies of their images shall be done in accordance with the details set out in this code. The request must fulfil a number of conditions:

1. Requests must be made using the appropriate form.
2. A fee of £10 must accompany the application.
3. Applications must be in person, accompanied with proper identification to prove the applicant's identity. This will usually be a passport or driving licence, or a birth certificate. Other forms of identification may be accepted at the discretion of the Data Controller.
4. Information must be provided by the applicant to assist the unit with locating those images
5. Images of other persons must be considered for blurring where it is decided by the data controller or his agent, that to release them to the subject applying might prejudice other person's privacy.
6. Images will not be released if their provision prejudices an investigation or interferes with the administration of justice.

Details of the form required and other details can be obtained from the Data Controller.

4 CCTV System

4.1 Introduction

The CCTV cameras in this system are connected into communications networks enabling individual cameras anywhere on the system to be monitored, controlled, and recorded by authorised personnel working for University of Bath Students' Union Event Control.

4.2 Key Personnel

4.2.1 System Manager

The University of Bath Students' Union Event Control scheme is managed locally by a manager with direct control of the scheme. The manager is responsible to the owner / hirer and has authority over the following:-

1. event control technician management;
2. observance of the policy and procedural practices;
3. release of data to third parties who have a legal right to copies;
4. control and security clearance of visitors;
5. security and storage of data;
6. security clearance of persons who request to view data;
7. release of new and destruction of old data and data medium, eg Images;
8. maintenance of the quality of the recording and monitoring equipment.

The system manager retains responsibility for the implementation of procedures to ensure that the system operates according to the purpose for which it was installed and in accordance with the objectives identified for the system.

The system manager has responsibility for the day-to-day liaison with all users of the system. This should include supervision of access to any data obtained by the system.

The system manager has a responsibility for the instigation of disciplinary procedures against users in matters relating to non-compliance with the code, operational procedures and breaches of confidentiality or the unauthorised release of data. This breach could lead to the instigation of criminal proceedings.

The manager is aware that if he or she acts outside the instructions of the data controller in relation to obtaining or disclosing the images, they may commit a criminal offence contrary to Section 55 of the 1998 Act, as well as breach their contract of employment.

4.2.2 Event Control Technician

The Event Control Technician has a responsibility to ensure that at all times the system is operated in accordance with the policy and all procedural instructions relating to the system, and for bringing to the immediate attention of the manager any matter affecting the operation of the system, including any breach or suspected breach of the policy, procedural instructions, security of data or confidentiality.

The Event Control Technician ensures that at all times users carry out their duties in an efficient and responsible manner, in accordance with the objectives of the scheme. This includes regular checks and audit trails to ensure that the documentation systems in place are working effectively. These systems include, for example:

- the image register;
- the users log;
- the incident log;
- witness statements; (as applicable)
- faults and maintenance records;
- the security of data;
- authorised visitors.

The Event Control Technician ensures that users carry out their duties in accordance with good practice and that they comply with Health and Safety requirements.

Event Control Technician are personnel located within the Event Control Room.

No visitors are to work without direct supervision (i.e. left continuously on their own monitoring cameras).

The integrity of a system depends very much upon the activities of the users, who should be completely trustworthy, and not only observe the civil rights of the public and individuals, but also respect their privacy.

Event Control Technicians have a responsibility to take appropriate action to deal with incidents detected by the camera, in accordance with the procedures laid down by the policy and then record such information as required by procedural instructions, in the appropriate log

Event Control Technicians should have a responsibility to bring to the immediate attention any defect of equipment or picture transmission that adversely affects the operation of the system.

Event Control Technicians should become proficient in the control of cameras and operation of all equipment forming part of the system. They should acquire a good knowledge of the area covered by the camera and ensure the information recorded or obtained by the system

is accurate, adequate, relevant and does not exceed that necessary to fulfil the purpose of the system.

4.3 Access to Event Control Room

4.3.1 General Access

Only visitors with a valid reason and who have prior authorisation from the system manager will be allowed access to University of Bath Students' Union Event Control CCTV system and monitoring areas. Public access to the monitoring and/or recording facility will be prohibited except for lawful, proper and sufficient reasons and only then with the personal authority of the system manager. Any such visits will be conducted and recorded in accordance with this code of practice. Authorised personnel will be allowed access to the Event Control Room to coordinate event operations.

4.3.2 Authorised Personnel Access

Authorised personnel include the following:

- University of Bath Students' Union Bars Manager
- University of Bath Students' Union Bars Supervisors
- University of Bath Students' Union Event Security Manager
- University of Bath Students' Union Event Security Personnel
- University of Bath Security
- University of Bath Students' Union Event Medical Co-ordinator

4.3.3 Police Access

Police Officers may be granted access to University of Bath Students' Union Event Control and monitoring areas for the purpose of retrieving evidence, advising on criminal intelligence, liaison and security purposes. Generally, the University of Bath Students' Union Event Control will be advised in advance of any visit, the reason for which must be authorised by an officer of the rank of Inspector or above unless special arrangements have been made.

The Police will have authorisation at Gold and Silver Command level to enter into the University of Bath Students' Union Event Control Room to take direct control, in times of:-

- Terrorism threats
- Reasons of national security
- Major incident co-ordination

4.3.4 Staff Access

Only trained and authorised personnel will be allowed access to monitor cameras.

4.3.5 Visitors' Book/Declaration of Confidentiality

ALL visitors will be required to sign a visitors' book. A template is included within the Procedural Manual. Visitors are required to make an undertaking that all information witnessed during their visit will be held as confidential. The visitors' book will act as a 'declaration of confidentiality'. The declaration of confidentiality will form part of the access notice before entering the University of Bath Students' Union Event Control Room or monitoring area. A copy of the declaration of confidentiality will be included within the visitors' book to remind visitors of their obligations. Standard templates are included in the Procedural Manual. The wording of the statement of confidentiality (declaration) will read:-

"In signing this visitors' book, all visitors to the University of Bath Students' Union Event Control Room acknowledge that the precise location of the University of Bath Students' Union Event Control Room and personal details of those operating the system, is and should remain, confidential. Visitors further agree not to divulge any information obtained, overheard or overseen during the visits."

Visitors will sign the visitors' book on arrival and enter the exact time of arrival and purpose of the visit. For security purposes, the car registration and company/organisation should also be entered. On departure the exact time will be inserted into the visitors' book.

By signing the visitors' book, visitors agree to abide by the confidentiality requirement of entry into the University of Bath Students' Union Event Control Room.

4.3.6 Event Control Room Physical Security

Authorised personnel will normally be present at all times when the equipment is in use. If the monitoring facility is to be left unattended for any reason (ie bomb threats/fired drills etc) the system will be locked and the room must be secured.

4.3.7 Log on Procedures

All staff using the system will be required to log on/off when the system is in use/not in use.

4.3.8 Documentation

Full records are maintained to ensure that there is a full audit trail and history relevant to procedures. This can be done manually or electronically. Log books or databases etc should be sequential so that entries cannot be overwritten or removed. Manually, they are to be completed in ink with mistakes and alterations clearly legible. Alterations should be initialled by the Systems Manager or supervisor.

The following logs and administrative documents are kept within the University of Bath Students' Union Event Control Room:-

(a) Visitors' Book
(b) Staff signing on/off

(c) Incident logs indicating details of time, date, location, nature, operator dealing and action taken
(e) Privacy zones, detailing where, for any reason, it is necessary to encroach on private areas that are not part of the contractual patrol (Data Protection Act).
(h) Image/CD, DVD viewing/copying register identifying who has viewed images CD. DVD, reasons and working copies made.
(j) Recorded audio register, detailing incoming/outgoing telephone calls and radio traffic.

4.3.9 Monitoring

Monitoring will be constant throughout the open time of the event.

Users monitor the cameras on the network on a proactive basis i.e. they will vary their activities in response to circumstances at the time, and intelligence provided by System Managers, Event Security, Medical Teams and the Police in preference to a fixed schedule.

4.3.10 Communications

A number of separate communication systems will be in operation within the University of Bath Students' Union Event Control Room. All systems are to be used strictly in accordance with operating procedures laid down by the suppliers/users.

In the event of an incident being observed by an Event Control Room Technician, contact will be made as per the procedures laid down in the operational manual by either by radio/telephone.

4.3.11 Analogue Recording and Image Administration

Video images recorded in the University of Bath Students' Union Event Control Room are only to be used under secure conditions for the following authorised purposes:-

Production in court of law for evidential purposes.
Production by University of Bath Students' Union for lawful purposes in connection with its statutory duties.

4.3.12 Recorded Material Management

4.3.12.1 General

University of Bath Students' Union Event Control is committed to the belief that everyone has the right to respect for his or her private and family life and their home. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information which the System gathers.

Arguably CCTV is one of the most powerful tools to be developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety. Equally, it may be regarded by some as the most potent infringement of people's liberty. If users,

owners and managers of such systems are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

After considerable research and consultation, the nationally acknowledged British Standards Institution CCTV Codes of Practice has been adopted as a template in the construction of this document.

For the purposes of this Code 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of The System, but specifically includes images recorded digitally, or on video image or by way of video copying, including video prints.

Every video or digital recording obtained by using The System has the potential of containing material that has to be admitted in evidence at some point during its lifespan.

It is therefore of the utmost importance that irrespective of the means of format (e.g., paper, copy, video image, digital image, CD or any form of electronic processing and storage) of the images obtained from the system, they are treated strictly in accordance with this Code of Practice from the moment they are received by the monitoring room until final destruction. Every movement and usage will be meticulously recorded.

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

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

Recorded material should be of the high quality required by the courts if it is to be admitted in evidence. It is essential, therefore, that recorded material evidence maintains total integrity and continuity at all times.

Appropriate security measures have been taken to prevent unauthorised access to, or alteration, disclosure, destruction, accidental loss or destruction of recorded material.

Hard copy prints or recorded material will not be released to organisations outside the ownership of the CCTV system other than for training purposes, or under guidelines referring to the release of information for the purposes of identifying alleged offenders or witnesses, in accordance with the University of Bath Students' Union Event Control Code of Practice.

A hard copy print is a paper copy of an image, which already exists on recorded material and should not be taken as a matter of routine. The person making the print is responsible for recording the full circumstances under which the print is taken, with reasons, in accordance with procedures. Ideally, each print should be allocated a unique number, which is recorded in the appropriate log.

If material is to be shown to witnesses, including police officers, for the purposes of obtaining identification evidence, it must be shown in accordance with the disclosure of data guidelines contained within this Code of Practice.

It may be beneficial to make use of 'real' video footage for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention and detection of crime. Any material recorded by virtue of The CCTV system will only be used for such bona fide training and education purposes.

4.3.12.2 General Processing Policy

All requests for the release of data shall be processed in accordance with this Code of Practice. All such requests should be channelled through the data controller. See page X above.

Every request for the release of personal data generated by this CCTV system will be channelled through the System Manager . The System Manager will ensure the principles contained within this Code of Practice are followed at all times.

In complying with the release of data to third parties, it is intended as far as reasonably practicable, to safeguard the individual's rights to privacy and to give effect to the following principles.

Recorded material shall be processed lawfully and fairly, and used only for the purposes defined in this Code of Practice;
Access to recorded material will only take place in accordance with the standards outlined in this Code of Practice;
The release or disclosure of data for commercial or entertainment purposes is specifically prohibited.

Members of the police service or other agency having a statutory authority to investigate and / or prosecute offences may, subject to compliance with this Code of Practice, release details of recorded information to the media only in an effort to identify alleged offenders or potential witnesses. Under such circumstances, full details will be recorded in accordance with the guidelines outlined within this document.

4.3.12.3 Recording Equipment

Recording equipment shall be checked regularly to ensure it is in good working order.

Equipment shall be subject of regular professional servicing.

Equipment will only be operated by a person who has proven ability or who has been trained. (If required an SIA CCTV Operator Licence will be held by an operator)

4.3.12.4 Quality

Good quality recording material and equipment is used as this significantly increases the chances of making a good recording.

Equipment used for making recordings is maintained in good working order. Regular and professional servicing is carried out, in accordance with the manufacturer's recommendations.

4.3.12.5 Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified. The Third, Fourth and Fifth Data Protection Principles are concerned with the quality of personal data. The standards to be met under this Code of Practice are set out below.

Video images used are good quality images to ensure compliance with (Third and Fourth Data Protection Principles).

4.3.12.6 Recorded Material (Processing of Images)

University of Bath Students' Union shall be regarded as the owner of recorded material including ownership of the copyright of any such material.

Images will be retained for no longer than is necessary (Fifth Data Protection Principle)

Once the retention period has expired, the images will be removed or erased (Fifth Data Protection Principle).

4.3.12.7 General Image Recorded Material

General image recorded material will be retained for 30 days, with images thereafter being recycled into normal usage.

All requests to view a recording should be made to the system manager who must ascertain that the request is legitimate and warrants access.

Imaged material may on occasions be used for training and demonstration purposes.

4.3.12.8 Evidential Images and Access Issues

If the images are retained for evidential purposes, they will be retained in a secure place to which access is controlled (Fifth and Seventh Data Protection Principles).

Once images have been determined to contain evidence, they will come under the rules of Criminal Justice System and be treated accordingly. In this respect, the Data Protection Act may not be applicable for disclosure purposes. (See exemptions to releasing Data)

No unauthorised access will be allowed to recorded video images containing evidence.

Access to recorded images is restricted to staff that need to have access in order to achieve the purpose(s) of using the equipment (Seventh Data Protection Principle).

All access to the medium on which the images are recorded should be documented (Seventh Data Protection Principle)

Access to the recorded images will be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the agreed documented disclosure policies (Seventh Data Protection Principle).

Once it is apparent that an image may contain material of evidential value, then it must be dealt with in accordance with the Operational guidelines. This may mean copied onto USB Flash Memory or archived for later copying or archiving into a separate hard drive area.

Original images will not be played to witnesses unless under the supervision of the Police or other agency

Copy images must only be made on authorised equipment and after an official request. A register of copies made will be maintained for audit purposes. (see Appendix E)

The first copy – the master copy, immediately after being copied, will be labelled, and sealed in a case and entered in the recording system (as an exhibit). This is in order to preserve its integrity in respect of any further evidential use.

A working copy of the master image will be made at the earliest opportunity. It is not practical to copy long periods of activity, except for serious offences. In most cases the copy image should cover the evidential section of the master image only (and 5 minutes either side).

Continuity of the use of all images, both master and copy from original recording and subsequent court viewing, must be accounted for with witness statements.

Requests from defence solicitors for copy images must be routed through the Crown Prosecution Service (CPS) and then the local Police Administration Support Unit. The CPS will advise on disclosure.

Where copying a master image takes place on behalf of defence, it should not be done without the authorisation of the CPS and a second copy will be prepared at the same time which will be forwarded to the CPS (to ensure they are aware of all materials disclosed to the defence).

No charge will be levied for the first copy of an image to the defence. Any subsequent copies may be charged for at the set charge.

Access to images may be provided in accordance with the release of images to third parties protocol. Usually this is in connection with civil disputes. A charge may be levied for any request.

On removing the medium on which the images have been recorded for the use in legal proceeding, the CCTV manager will ensure that they have documented:

1. The date on which the images were removed from the general system for use in legal proceedings.
2. The reason why they were removed from the system.
3. Any crime incident number to which the images may be relevant.
4. The location of the images

For example - if the images were handed to a Police Officer for retention

The signature of the collecting Police Officer, where appropriate. (Third and Seventh Data Protection Principles).

4.3.12.9 Viewing of Images

Facilities may be provided to enable evidential images to be viewed by authorised persons.

Viewing of images for identification must be considered against all the issues relevant to the subject of identification.

Viewing of the recorded images will take place in the reviewing suite or other secure environment not open to general viewing. Other employees should not be allowed to have access to that area when a viewing is taking place (Seventh Data Protection Principle).

Removal of the medium on which images are recorded, for viewing purposes, is documented as follows:

(a) The date and time of removal
(b) The name of the person removing the images
(c) The name(s) of the person(s) viewing the images. If this should include third parties, this includes the organisation of that third party
(d) The reason for the viewing
(e) The outcome, if any of the viewing
(f) The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

All users and employees with access to images should be aware of the procedure which needs to be followed when accessing the recorded images (Seventh Data Protection Principle).

Monitors displaying images from areas in which individuals would have an expectation of privacy cannot be viewed by anyone other than the authorised employees or the user of the equipment (Seventh Data Protection Principle).

4.3.12.10 Video Prints

A video print is a copy of an image or images which already exist on video image / computer disc. Such prints are equally within the definitions of 'data' and recorded material. (eg still photograph from images of live incidents)

Video prints will not be taken as a matter of routine. Each time a print is made it must be capable of justification by the originator who will be responsible for recording the full circumstances under which the print is taken in accordance with this Code of Practice.

Video prints contain data and will therefore only be released under the terms of this Code of Practice, under 'Release of data to third parties'. If prints are released to the media, in an effort to identify alleged offenders or potential witnesses, full details will be recorded in accordance with this Code of Practice.

A record will be maintained of all video prints taken. The recorded details will include:

- a sequential number,
- the date,
- time and location of the incident,
- date and time of the production of the print and the identity of the person requesting the print., (if relevant)
- and the purpose for which the print was taken. (Appendix)

The records of the video prints taken will be subject to audit in common with all other records in the system.

All users will be trained in their responsibilities under this Code of Practice in respect of copying; they should be aware of:

A. The user's security policy e.g., procedures to have access to recorded images.
B. The user's disclosure policy. See the section on access to and disclosure of images to third parties.
C. Rights of individuals in relation to their recorded images.

4.3.13 Recorded Material Register

4.3.13.1 Image Register

There should be a register documenting the complete life of each image from the time of its creation up to and including any presentation at court as an exhibit until its destruction. The principle of such a register is to show the life of the image at all stages whilst in the owner's possession. It is essential that integrity and continuity be maintained. Such a register may also show itself to be useful to enable evaluation of the video security installation, as it will

contain information relating to the number of images and cases where video evidence is obtained.

The register should ideally be a bound book with printed, numbered pages to prevent loose-leaf pages being removed and/or replaced. Before use each image should be indelibly marked, ideally on the body, with a unique reference number.

Each image medium will have a unique tracking number/record maintained in accordance with this Code of Practice which will be retained for at least three (3) years, after the image has been destroyed. The tracking record shall identify every use and person who has viewed or had access to the image since the initial breaking of the seal to the destruction of the image.

The register should include the following:

A. unique image reference number
B. image type
C. time/date/person placing image in store
D. time/date/person removing from secure storage for use
E. time/date/person returning image to secure storage after use
F. remarks column to cover additional points, for example: erase/ destroy/handed over to police/removed from recording machine
G. time/date/person responsible for any subsequent removal of the image
H. time and date of delivery to the police, identifying the police officer concerned
I. time/date/person responsible for erasure and/or destruction

4.3.13.2 Making Recordings

The following procedure will be followed:

A. Before recording, test that all equipment is working efficiently.
B. Check time/date selection is correct.
C. Record image identification URN.
D. Maintain records of the operator(s) of the equipment. This enables the manager to establish who was operating the equipment at any given time.
E. Record without interruption, wherever practicable. Any interruption should be recorded.
F. On completion of the recording, remove and file appropriately the image from the recorder.

Images will then be returned to secure storage, and recorded in the image register.

4.3.13.3 Incident Policy

The day to day operation of the system will be recorded in a Incident Book which will be a hard backed A4 book. This will include issues that are not considered Incidents but require

the details to be noted down. Examples of what should be recorded include but are not restricted to;

- Visitors to the room – Police etc
- Change of operators and breaks from screen
- Minor events, such as a request to monitor traffic flow or specific persons entering a building
- etc.

In the event of an incident being observed by a CCTV operator, action will be taken in accordance with local procedures. Refer to any Manual of Guidance or Assignment Instructions.

An incident is defined as an unusual occurrence requiring more than just a routine response and requiring additional resources to be deployed.

A record of all incidents will be maintained by users in the appropriate incident log. The information to be recorded will include anything of note that may be useful for investigative and evidential purposes or future system assessment and evaluation.

4.3.13.4 Who makes the response?

The Operational Procedures- Assignment Instructions identify who should be responsible for making the response to an incident. Depending on the incident, this may be:-

- Event Security
- Campus Security
- Bars Managers
- Medical First Responders
- Backstage
- Police
- Other nominated personnel

4.3.13.5 Intrusive Surveillance

Intrusive Surveillance is where a device or person is placed in or on the subject property or vehicle. This type of surveillance WILL NOT be carried out by University of Bath Students' Union Event Control.

Appendix A

Human Rights Information

Human Rights Information

University of Bath Students' Union Event Control will observe and is bound by the Human Rights Act 1998. The outline of the articles applicable to CCTV are produced below;

Article 3 - Prohibition of Torture (Absolute)
The right not to be subjected to **inhuman or degrading treatment** which may be defined as using cameras to follow females closely or zoom in to certain parts of the female anatomy.

Article 6 – Right to a Fair Trial (Absolute)
The right to a **fair trial.**

- the right to a *fair* hearing - the right to a *public* hearing - the right to a hearing before an *independent and impartial tribunal* - the right to a hearing *within a reasonable time*. Evidence collected by CCTV will be available to any defence.

Article 8: Privacy Issues (Qualified)

Everyone has the right to respect for his or her private family life, home and correspondence.

There can be no interference **except** in accordance with the law:

- is necessary in a **democratic society**
- in the interests of **national security**,
- **public safety** or
- the **economic well being of the country**,
- for the prevention of **disorder** or **crime**,
- for the protection of **health or morals**,
- or for the protection of the **rights and freedoms of others**.

Article 10 –Freedom of Expression (Qualified)

- The right to hold opinions and express views,
- however unpopular or disturbing.
- May only be restricted in certain circumstances

Article 11 – Freedom of Assembly & Association (Qualified)

- The right to assemble with other people in a peaceful way.
- The right to associate with other people
    - Including the right to form a trade union.
- These rights may be restricted only in specified circumstances.

Article 14 Prohibition of Discrimination (Qualified) – to be applied to all Rights

- Prohibition of **<u>Discrimination</u>**
    - on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.
- *Everyone has equal rights whatever their status*

Appendix B

Data Protection Act

Data Protection Act 1998

The Data Protection Act 1998 sets out 8 principles for the processing of personal data. These are outlined as follows:

1. **Data must be processed fairly and lawfully,**
2. **processed for limited purposes, specified and lawful**
3. **adequate, relevant and not excessive, -** *relates to positioning of cameras*
4. **accurate and up to date**
5. **not kept for longer than is necessary,**
6. **processed in accordance with individuals rights, -** *subject access rights £10 etc*
7. **kept secure, -** not released, destroyed etc without proper authority
8. **not transferred to non EEA countries without appropriate protection.**

More information can be obtained from University of Bath Students' Union Event Control and any request to have a copy of your data can also be obtained.

Appendix C

The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIPA)

This legislation deals with using CCTV in a covert manner. It is very unlikely that CCTV operated by University of Bath Students' Union Event Control will be used in a covert manner. However, if it is requested, any request must fulfil the legal requirements of having a proper authorisation and be proportionate to what is being undertaken.

An example might be where the Police request a vehicle to be covertly observed using public space cctv as part of a pre-planned or ongoing investigation. This would require a properly authorised request as it is not an immediate response to the event.

Authorisations will be treated as confidential due to the nature of the activity. This process is overseen by the Government's Surveillance Commissioners, who audit this procedure regularly and publish a report.

Further information can be obtained from the Surveillance Commissioners;

www.surveillancecommissioners.gov.uk/

Appendix D

Authorisation for the release of digital media

AUTHORISATION FOR THE RELEASE OF DIGITAL MEDIA

To be completed when digital evidence has been requested from the event control room.

Incident Details

Date of Incident	
Time of Incident	
Location of Incident	
Description of Incident	

Request Detail

Date of Request	
Requested by	
Reason for Request	
Requestor has viewed media?	YES / NO

Digital Media Information

DVR Number - Channel Number	
Media File Name	
Media Type & Serial Number	
Media Time of Incident Occurring	
Timecode Time of Incident Occurring	
Are other individuals identifiable?	YES / NO
Total Media Length	

Released by

Operator's Name	
Operator's Signature	
Date of release	

Received by

Receiver's Name	
Receiver's Signature	
Date of receipt	

Appendix E

Digital media release log

AUTHORISATION FOR THE RELEASE OF DIGITAL MEDIA LOG

Date of Request	Date of Incident	Time of Incident	Location of Incident	DVR Number	Channel Number	Media File Name	Timecode Time of Incident	Media Serial Number	Media Type	Requestor's Nam	Operator's Nam	Receiver's Name

Appendix F

Control Room Visitors Log

Control Room Visitors Log

In signing this visitors' book, all visitors to the Event Control room acknowledge that the precise location of the Event Control room and personal details of those operating the system, is and should remain, confidential. Visitors further agree not to divulge any information obtained, overheard or overseen during the visits.

Date	Time In	Name	Purpose of Visit	Signature	Time Out

Appendix G

Control Room Standard Operating Procedures

Event Control
Standard Operating Procedure
Evacuation (Founders Sports Hall)

Purpose

To provide guidance on how the event control room operators should respond to a an evacuation of the Founders Sports Hall.

Procedure

THE CONTROL ROOM OPERATORS SHOULD NOT PUT THEMSELVES OR OTHERS IN DANGER. SHOULD THE CONTROL ROOM OPERATORS AT ANY POINT FEEL THAT THEIR HEALTH AND SAFETY MAY BE COMPROMISED BY REMAINING IN THE CONTROL ROOM THEY SHOULD EVACUATE BY THE NEAREST EMERGENCY EXIT.

1. All non-essential personnel should leave the control room immediately by the nearest emergency exit.
2. If it is safe to do so the Event Control Room should monitor the evacuation of the Founders Sport Hall.
3. The evacuation should be registred in the Event Log.
4. If it is safe to do so the Event Control Room should attempt to identify the reason for the evacuation via the CCTV system.
5. Further information should be added to the event log as it becomes available.
6. Event Control should make security and technical teams aware of the situation if the reason for evacuation is easily identifiable.
7. Event Control should monitor the egress points of the Founders Sports Hall via the CCTV system. If required additional security should be dispatched where identified
8. Once evacuation of the Founders Sports Hall is complete;
    a. The Event Control Room should switch off all monitors and projectors.
    b. Recording equipment should be locked.
    c. The Event Log and Visitors Log should be taken to the allocated Rendezvous Point.
    d. Once all personnel have left the Event Control Room Dimmer lighting and all non-essential power supplies should be switched off.
9. The incident should be marked as closed in the event log once the building is declared safe and security has given clearance for return the building.

Event Control
Standard Operating Procedure
Event Evacuation

Purpose

To provide guidance on how the event control room operators should respond to the complete evacuation of the eventl.

Procedure

THE CONTROL ROOM OPERATORS SHOULD NOT PUT THEMSELVES OR OTHERS IN DANGER. SHOULD THE CONTROL ROOM OPERATORS AT ANY POINT FEEL THAT THEIR HEALTH AND SAFETY MAY BE COMPROMISED BY REMAINING IN THE CONTROL ROOM THEY SHOULD EVACUATE BY THE NEAREST EMERGENCY EXIT.

1. All non-essential personnel should leave the control room immediately by the nearest emergency exit.
2. If it is safe to do so the Event Control Room should monitor the evacuation of the Event.
3. The evacuation should be registred in the Event Log.
4. If it is safe to do so the Event Control Room should attempt to identify the reason for the evacuation via the CCTV system.
5. Further information should be added to the event log as it becomes available.
6. Event Control should make security and technical teams aware of the situation if the reason for evacuation is easily identifiable.
7. Event Control should monitor the egress routes and points of the Founders Sports Hall and the Event via the CCTV system. If required additional security should be dispatched where identified
8. Once the evacuation of the Event is complete;
    a. The Event Control Room should switch off all monitors and projectors.
    b. Recording equipment should be locked.
    c. The Event Log and Visitors Log should be taken to the allocated Rendezvous Point.
    d. Once all personnel have left the Event Control Room Dimmer lighting and all non-essential power supplies should be switched off.
9. The incident should be marked as closed in the event log once the event is declared safe and security has given clearance for return the building.

Event Control
Standard Operating Procedure
Security Incident

Purpose

To provide guidance on how the event control room operators should respond to a minor security incident.

Procedure

1.
    a. If the Event Control Room observes any activities that require attendance by event security personnel or other criminal activity this should be recorded in the event log and brought to the attention of the security officer in the control room.
    b. If the incident is identified by security personnel and relayed to the control room the activity should be recorded in the event log.
2. A camera covering the incident should then be displayed on the video wall, and the incident monitored closely until security personnel arrive.
3. Once security personnel are at the incident it should be monitored closely to provide further assistance if required.
4. Further information should be added to the event log as it becomes available.
5. Event Control should dispatch any other required personnel such as medical or technical teams as required.
6. Event Control should request campus security / police if required.
7. The incident should be marked as closed in the event log once security personnel have left the scene and any perpetrators / victims dealt with.

Event Control
Standard Operating Procedure
Report of Fire

Purpose

To provide guidance on how the event control room operators should respond to the report of a fire.

Procedure

THE CONTROL ROOM OPERATORS SHOULD NOT PUT THEMSELVES OR OTHERS IN DANGER. SHOULD THE CONTROL ROOM OPERATORS AT ANY POINT FEEL THAT THEIR HEALTH AND SAFETY MAY BE COMPROMISED BY REMAINING IN THE CONTROL ROOM THEY SHOULD EVACUATE BY THE NEAREST EMERGENCY EXIT.

1.
    a. If the Event Control Room observes a fire this should be recorded in the event log and brought to the attention of the security officer in the control room.
    b. If the report of fire is identified by other personnel and relayed to the control room the fire should be recorded in the event log.
2. A camera covering the reported fire should then be displayed on the video wall, and the incident monitored closely until security personnel arrive.
3. Once security personnel are at the incident it should be monitored closely to provide further assistance if required.
4. Further information should be added to the event log as it becomes available.
5. Event Control should dispatch any other required personnel such as medical or technical teams as required.
6. Event Control should request campus security / fire brigade if required.
7. The incident should be marked as closed in the event log once security personnel have left the scene and it is declared safe.

Event Control
Standard Operating Procedure
Fire Alarm (Founders Sports Hall)

Purpose

To provide guidance on how the event control room operators should respond to a fire alarm in the Founders Sports Hall.

Procedure

THE CONTROL ROOM OPERATORS SHOULD NOT PUT THEMSELVES OR OTHERS IN DANGER. SHOULD THE CONTROL ROOM OPERATORS AT ANY POINT FEEL THAT THEIR HEALTH AND SAFETY MAY BE COMPROMISED BY REMAINING IN THE CONTROL ROOM THEY SHOULD EVACUATE BY THE NEAREST EMERGENCY EXIT.

1. All non-essential personnel should leave the control room immediately by the nearest emergency exit.
2. If it is safe to do so the Event Control Room should monitor the evacuation of the Founders Sport Hall as defined in the Standard Operating Procedure - Evacuation (Founders Sports Hall).
3. The alarm should be registred in the Event Log.
4. If it is safe to do so the Event Control Room should attempt to identify the source of the fire alarm via the CCTV system.
5. Further information should be added to the event log as it becomes available.
6. Event Control should make security and technical teams aware of the situation if the source of the alarm is easily identifiable.
7. Once evacuation of the Founders Sports Hall is complete;
    a. The Event Control Room should switch off all monitors and projectors.
    b. Recording equipment should be locked.
    c. The Event Log and Visitors Log should be taken to the allocated Rendezvous Point.
    d. Once all personnel have left the Event Control Room Dimmer lighting and all non-essential power supplies should be switched off.
8. The incident should be marked as closed in the event log once the building is declared safe and security has given clearance for return the building.

Event Control
Standard Operating Procedure
Medical Incident

Purpose

To provide guidance on how the event control room operators should respond to a medical emergency.

Procedure

1.
    a. If the Event Control Room observes any incidents that require attendance by event medical personnel this should be recorded in the event log and brought to the attention of the medical dispatcher in the control room.
    b. If the incident is identified by site personnel and relayed to the control room the incident should be recorded in the event log.
2. Medical Response:-
    a. The medical dispatcher should then report whether a medical team is available to attend and whether they have been dispatched.
    b. If a medical team is unavailable and the patient only had a minor injury they should be asked to make their way to the nearest first aid post.
    c. If a medical team is unavailable and the patient is unable to make their way to a first aid post the incident should be assessed as whether external medical assistance is required.
3. A camera covering the incident should then be displayed on the video wall, and the incident monitored closely until medical personnel arrive.
4. Once medical personnel are at with the patient it should be monitored closely to provide further assistance if required. Medical team arrival should be recorded in the event log.
5. Further information should be added to the event log as it becomes available.
6. Event Control should dispatch any other required personnel such as security as required.
7. Event Control should request campus security / ambulance if required.
8. The incident should be marked as closed in the event log once the patient is in the care of the medical team and no further action is required..

Appendix H

Image Register

IMAGE REGISTER

Image Ref Number	Image Type	Image Timecode	Captured / Saved		Removed from Storage		Remarks	Received By		Erased / Destroyed	
Date-Time-DVR No.-Channel N			Person	Time & Date	Person	Time & Date	Erased / Destroyed / Printed / Handed to Police	Person	Time & Date	Person	Time & Date