Mid Essex Hospital Services NHS
NHS Trust

CCTV Policy	**Type: Policy** **Register No: 10094** **Status: Public**
Developed in response to:	NHSLA requirement, Serious Incident Management Improve Governance Data Protection Act 1998
Contributes to CQC Core	Outcome 10

Consulted With	**Post/Committee/Group**	**Date**
Clive Edwards	Staffside Representative	June 2014
Sue Brown	Head of Hotel Services	June 2014
Eric Carter	Portering and Security Manager	June 2014
Kate Thomson	IT Manager	June 2014
Ryan Curtis	Health, Safety & Security Manager	June 2014
Helen Clarke	BNHSLA Audit Co-ordinator	June 2014
Liz Stewart	Information Governance Manager	June 2014
Professionally Approved By	Carin Charlton, Director of EFM	June 2014

Version:	3.4
Issuing Directorate:	Estates & Facilities Management
Ratified by:	Document Ratification Group
Ratified on:	26th June 2014
Trust Executive Sign Off Date:	July 2014
Implementation Date:	7th July 2014
Next Review Date:	Extension agreed to September 2019
Author/Contact for Information:	Doug Smale, LSMS
Policy to be followed by (target staff):	All staff & Trust users
Distribution Method:	Intranet & Website
Related Trust Policies (to be read in conjunction with):	Violence & Antisocial Behaviour Security Policy Risk Management Policy & Strategy Lone Worker Policy Missing Patients Policy Safeguarding Children & Young People 0-18 Policy Safeguarding Vulnerable Adults Policy

Document History

Review No	**Reviewed by**	**Issue Date**
1.0	Jim Dorrian	October 2010
2.0	Doug Smale - updates of roles and responsibilities and policy extension	Nov 2012
3.0	Doug Smale - formal review	June 2014
3.1	Doug Smale - updated regarding 31 day recording 13.9	30 March 2015
3.2	Doug Smale Extended for standardisation and review process (Success Regime)	21 November 2017
3.3	Jo Mitchell - 6 month extension request due MSB standardisation	6th November 2018
3.4	Jo Mitchell - 4 month extension request due MSB standardisation	29th May 2019

CONTENTS

1. Purpose

1.1 The purpose of this policy is to ensure that where Controlled Circuit Television (CCTV) is used on Trust premises, that it is not misused or abused, it is correctly and efficiently installed and operated, and the use of it adheres to the principles of the Data Protection Act 1998, Human Rights Act 1998 and Regulation of Investigatory Powers Act 2000.

2. Introduction

2.1 This policy outlines the appropriate actions and procedures regarding CCTV systems so that they are correctly and efficiently installed, operated and maintained. In addition to this, CCTV footage is to be correctly stored and recorded, in a manner that will secure the consistent effectiveness of the CCTV system. This will be carried out so the CCTV system is not abused or misused while preserving the civil liberty of law abiding citizens at all times. In developing this policy, due account has been taken of the following guidance and strategies:

- The CCTV Code of Practice produced by the Information Commissioner. http://www.ico.gov.uk/for_organisations/data_protection/topic_guidea/cctv.aspx
- Caldicott Report 1997
- Information Governance Strategy
- Data Protection Act 1998

3. Scope

3.1 The policy is binding on all employees of the Trust and applies also to other persons who may, from time to time, and for whatever purpose, be present on any of its premises and whose images may be captured by the CCTV system.

4. Policy Statement

4.1 No CCTV scheme should be initiated, installed, moved or replaced without prior approval by the Caldicott Guardian (Medical Director), or someone delegated to approve such schemes. The Data Protection Officer (Information Governance Manager) must also be informed.

4.2 All schemes will be monitored and managed using the following procedures and must be formally approved (as above) prior to any installation.

- Local Security Management Specialists (LSMS) will assess the appropriateness of and reasons for, using CCTV or similar surveillance equipment in accordance with the CCTV Code of Practice.
- The assessment process and the reasons for the installation of the scheme will be clearly documented.
- Assessment / findings will be shared with the Directorate involved.

4.3 The Trusts CCTV system and images collected are solely for the purpose of the prevention and detection of crime. Images should not be requested or made available for any other reason involving Trust business without consultation with the Trust's Security Management Director (SMD) and LSMS. Only the SMD and LSMS can give permission for images to be accessed outside of the reasons of prevention or detection of crime.

4.4 If however, while CCTV images are being viewed for the prevention and detection of crime, CCTV operatives see something that cannot be expected to be ignore, such as other criminal activity, gross misconduct, or behaviour which puts others at risk, this should be immediately reported to the SMD and LSMS to allow such images to be used to further investigate the inadvertently viewed incidents.

5. Definitions and Abbreviations

- **ACPO:** The Association of Chief Police Officers.
- **CCTV Operator:** the person who is responsible for watching, controlling and recording the pictures produced by CCTV cameras. Those people will consist of the Security Management Director, Local Security Management Specialist, Hotel Services Manager, Portering Security Manager and Security Officers.
- **CCTV:** Closed Circuit Television.
- **Control Room:** CCTV Control Room facility within Zone A.
- **DRF:** Digital Recording Facility
- **EP:** Essex Police.
- **Evidential Material** and **Unused Material:** shall be a deemed to be as defined under PACE.
- **LSMS:** Local Security Management Specialist who is nationally accredited and has responsibility for all security issues within an NHS Trust.
- **NHS CFSMS:** National Health Service Counter Fraud Security Management Services and they have policy and guidance responsibility for security management issues within the NHS.
- **PACE:** The Police and Criminal Evidence Act 1984.
- **Recorded material:** referred to in this policy shall include, but is not limited to, video tape, compact disc, computer disc, film, DVD, or any other media used for storing images, which can be viewed or processed after the event. Under NO circumstances shall any CCTV System be permitted to monitor or record audio information. Recorded material shall be divided into the categories of Evidential Material or Unused Material.
- **SMD:** Security Management Director

6. Roles and Responsibilities

6.1 Chief Executive

The Chief Executive is responsible for ensuring that this policy is implemented throughout the Trust and has a nominated Security Management Director (SMD).

6.2 Director of Estates & Facilities Management

The Director of Estates & Facilities Management is the nominated Security Management Director (SMD) for the Trust.

6.3 Medical Director

The Medical Director is the Trust appointed Caldicott Guardian and is the devolved strategic executive lead for the management of patient information and security. The Guardian's key responsibilities are to oversee how staff use personal health information and ensure that patients' rights to confidentiality are respected. In addition assure the Trust Board that all security measures are in line with national guidance and legislation.

6.4 Local Security Management Specialist (LSMS)

The LSMS is nationally accredited by the NHS CFSMS to implement the Secretary of State for Health Directions to ensure that an environment is safe and secure. This will allow for a safe working environment for staff where the highest standards of clinical

care can be made available to patients. The Portering and Security Manager and/or LSMS, are also the data controller of CCTV images and is responsible for ensuring that the viewing of images whilst investigating security related incidents is conducted in a controlled area and that images are only released to appropriate bodies in connection with the investigation, prosecution or prevention of crime under the guidance of the Police and Police and Criminal Evidence Act criteria.

6.5 **Head of Hotel Services**

The Hotel services Manager has a duty for the following.

- the overall development and management of the CCTV system
- ensuring that the Trust that all developments are undertaken in a consistent manner
- ensuring that additional CCTV cameras are only installed in accordance with appropriate legislation

6.6 **Portering and Security Manager**

The Portering & Security Manager will ensure that:

- designated Security Officers who use the CCTV equipment appropriately trained in using the systems
- the CCTV control room facilities are operational
- CCTV control room is secured at all times and has systems in place to record who enters the room
- a maintenance contract is in place and is being undertaken to satisfactory standards

6.7 **Designated Security Officers/CCTV Operators**

The Security Officers that are designated are responsible for ensuring that:

- only those authorised to access the CCTV are authorised to do so and that details of those that access the CCTV control room are recorded (as per appendix 3).
- details of any requests made to access CCTV that is not in accordance with this policy are escalated to the Portering & Security Manager
- report any faults with the CCTV system to the Portering & Security Manager immediately at point of identifying the fault

7. CCTV Purpose

7.1 The Trusts CCTV system and images collected are solely for the purpose of the prevention and detection of crime. Images should not be requested or made available for any other reason involving Trust business without consultation with the Trust's Security Management Director (SMD) and LSMS. Only the SMD and LSMS can give permission for images to be accessed outside of the reasons of prevention or detection of crime.

7.2 If however, while CCTV images are being viewed for the prevention and detection of crime, CCTV operatives see something that cannot be expected to be ignore, such as other criminal activity, gross misconduct, or behaviour which puts others at risk, this should be immediately reported to the SMD and LSMS to allow such images to be used to further investigate the inadvertently viewed incidents.

8. CCTV System

8.1 CCTV System Description

- Pan, Tilt and Zoom (PTZ) and static cameras are generally provided within the CCTV monitor areas covered by this Code of Practice and, depending upon their location and purpose, these will be either pole or building mounted.
- CCTV Control Room equipment consists of a main bank of television monitors, controlling unit and a controller's desk. The station has been fitted with an agreed amount of dedicated television monitors and a digital recording system, which incorporates keyboard and joystick control devices.
- The CCTV Control room is located in the Security Officer's room where pictures are received, controlled and monitored from CCTV systems covering car parks and internal areas within the Trust.
- The CCTV Control Room will not be permanently staffed by trained Security Officers but rather as and when necessary.
- Day to day management, co-ordination and overseeing of the security officers will be undertaken by the Duty Supervisor who is directly responsible to the Portering Security Manager.
- CCTV images can be viewed by the Portering Security Manager via a PC link in their office thus being classed as a CCTV operator.

8.2 CCTV Operators

- Security officers operating the CCTV system shall be appropriately trained to Security Industry Authority level.
- All operators of CCTV equipment will be trained in their responsibilities in accordance with the Trust's CCTV policy and Code of Practice.
- All staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

8.3 Maintenance of the CCTV Systems

- The CCTV system shall be maintained to a high standard of operating efficiency using experienced and competent specialist maintenance engineers. The Portering Security Manager shall keep a record of all routine maintenance carried out to the system(s) including the quality of such maintenance.
- No part of the system shall be left inoperative for any reason, other than for the purpose of its maintenance or repair and all such works must be carried out expeditiously. All repairs to the system shall be carried out at the earliest possible and reasonable time on becoming aware of any fault or defect. This system will be backed up through IT and be linked to the generator back up system.

9. Compliance with the CCTV Code of Practice

9.1 CCTV operators and users of the CCTV systems shall be required to give a formal undertaking that they will comply with the CCTV Code of Practice and act in good faith with regard to the basic principles which it embodies.

9.2 All such CCTV operators and users shall comply with this requirement by signing a copy of a CCTV Code of Practice Compliance Declaration. The originals of all such declarations shall be retained for safe keeping by the Security Manager with a copy kept in staffs personal files.

9.3 The connection of additional CCTV systems to the Control Room will be permitted only if they comply with the following criteria:-

- They satisfy the technical criteria and standards required by the Trust.
- The camera locations have been approved by the Security Manager and LSMS in respect of settings that are permitted under this policy.
- System owners agree to comply with the CCTV Code of Practice
- System owners agree to maintain the system in accordance with the requirements set out in the CCTV Code of Practice.

10. Control Room Operations and Management

10.1 Control Room Operations & Procedures

- All contracted security staff working within the CCTV Control Room will conform to the CCTV Code of Practice.
- Only personnel who are fully trained or under supervised training in the use of the systems monitoring equipment, communication systems and the operational and management procedures required under this Code of Practice will be permitted to undertake duties within the Control Room.
- In the case of a major incident or for other purposes approved by and at the discretion of the LSMS, the control of the CCTV Control Room may be transferred to police personnel for the duration of any such incident or for a period agreed by the LSMS.
- Pictures from all cameras must be recorded at all times. Viewing live pictures without recording will not be permitted.
- Camera view selection will be governed by prioritised operational criteria developed from activity and incident data.

10.2 Access to the CCTV Control Room

- Security of the CCTV Control room shall be maintained at all times.
- Only those persons with a legitimate purpose will be permitted access to the CCTV Control Room
- Access to the Control Room will be restricted to authorised personnel, equipment maintenance engineers, the LSMS and other authorised Trust staff. A list of authorised persons will be displayed within the CCTV control room as agreed by the Head of Hotel Services and LSMS and kept available for inspection by CCTV Independent Inspectors in accordance with the CCTV Code of Practice.
- A CCTV Control Room Key Register is maintained in order to record anyone the key for the room is issued to (as seen in appendix 2).
- Police and visitors access to the CCTV Control room will be by prior arrangement with and by the authorisation of the Security Manager or LSMS or such other trained staff who may be delegated to assume responsibility for her/his duties, from time to time.
- Access for the purpose of cleaning and general repairs will be permitted but only under the direct supervision of CCTV Control Room personnel. The CCTV Control Room Key Register is completed for this access.
- The Independent Inspectors under the Code of Practice may visit the Control Room without prior appointment.
- Records shall be kept of all access to the control room, including the details of the individuals concerned, the reason for their access, their time of arrival and their time of departure (as seen in Appendix 3).

11. Camera Positioning

11.1 General Principles

- Cameras will be sited in positions which are clearly visible to patients, visitors and staff. Signs shall be prominently displayed in order to inform the public that CCTV is operating.
- The setting of cameras will be subject to the agreement of the Portering Security Manager/LSMS.
- As far as is reasonably practicable; all cameras should be sited in positions, which will minimise their susceptibility to criminal damage.

11.2 Privacy

- Except for wide angle or long distance observation, views into residential premises and office accommodation shall be excluded from the field of vision of all cameras.
- Close up views into windows of living accommodation is strictly prohibited.

11.3 Covert CCTV (Directed Surveillance)

- The use of covert CCTV if required must be requested through the police in accordance with PACE/RIPA. If the police refuse then authority can only be given by the NHS Security Management Services.

12. Reporting and Evaluation

12.1 Records

- All significant activities, operations, incidents and occurrences in the CCTV Control Room together with those relating to the operation and monitoring of the CCTV systems shall be recorded in a logical and presentable form.
- CCTV Control Room Operational Records shall include the following
    - CCTV Control Room Key Register - Appendix 2
    - CCTV Control Room Access Register - Appendix 3
- The majority of the above information shall be recorded in a specific log to prevent administration and potential for error.
- All security incidents are to be reported inline with the Trust incident reporting procedures.
- Visitor logs shall be kept of all authorised personnel visiting the CCTV Control Room (see appendix 2 and 3).
- With the exception of 'Recorded Material' storage which is covered separately in Section 12, all Control Room Operational Records shall be kept in the Control Room for 12 months and for at least a further two years in secure storage before being destroyed.

12.2 Independent Inspection (Acting for DPA Commissioner)

Independent Inspectors are persons who have undergone Police vetting and verification procedures. They are permitted access to the Control Room at any time, giving 7 days notice. They have the authority to check the identity and authorisation of any person in the Control Room and to examine all logs, video and photographic material with the exception of any evidential tapes which may be stored under seal and which would require prior approval of the police before viewing in accordance with the stipulated viewing procedures.

13. Recorded Material

13.1 Storage and Identification

- General recorded material not required for evidential purposes or for subject access will be retained as described in 9.2 and will then be automatically overwritten.

- The CCTV Access Register (see Appendix 3) records the time and date of each DVD created from CCTV and the areas covered by the recorded material. The register will record who the DVD is used to, the reason for the DVD being requested and the individual who is responsible for its safe keeping.
- Each DVD will be identified by a sequential number and will be fully referenced.
- Original DVD recordings (other than the copy taken by the police) will not be permitted to be removed from the CCTV Control Room because its continuity, correct storage and handling cannot be assured or verified.

13.2 **Access and Copying of Recorded Material**

- Statutory prosecuting authorities will be permitted to view CCTV footage within the Control Room. In the case of any recording which is deemed to contain evidential material, the statutory prosecuting authority will be permitted to remove recorded image(s) from the CCTV Control Room including any working copy of the DVD.
- Statutory Prosecuting Agencies (CPS and Police) together with the public will be permitted access to recorded material where it is necessary for the investigation and detection of a particular offence or offences or for the prevention of crime or where required under the Police and Criminal Evidence Act 1984 (PACE) and the Regulation of Investigatory Powers Act 2000 (RIPA).
- When removing image recordings, if it is needed in legal proceedings continuity of evidence is essential. The operator must ensure that the following is documented:
    - The date the images were removed for this purpose
    - The name of the person who removed the images
    - The name(s) of those viewing the images (if this includes a third party, the organisation name should be recorded)
    - Why the images were removed
    - The crime reference/incident number, if known
    - The outcome, if any, of the viewing
- A CCTV witness statement must be completed whenever a recording is handed over to the police or any other person who intends to use it as evidence. The purpose of the witness statement is not to describe the events shown on the recording, but to verify the continuity of evidence chain. If the police or other organisation requires the original recording (digital hard drive) consideration should be given to making a copy which should be retained.
- Any initial review of recorded material must take place by the Portering Security Manager/LSMS so that an assessment as to whether or not it is Evidential or Unused Material can be made. The only exception to this shall be in instances where for technical or scientific reasons an 'off site' review is required but in all such instances the written authorisation of the Portering Security Manager/LSMS shall be required prior to release of the recorded material.
- Viewing of evidential material by defendants and their appointed solicitors shall be carried out “off site” under the control of the prosecuting authority's investigating officer. It will be the responsibility of the prosecuting authority to provide working copies of any such material to defendants or their appointed solicitor

13.3 **Public Access**

- There shall be no public access to taped material other than in connection with the investigation, prosecution or prevention of crime under the guidance of the Police and Police and Criminal Evidence Act and Data Protection Act criteria.
- In the event that the Police make a request to have access to CCTV footage that they require in relation to investigations or potential prosecutions in relation to national security, actual or potential terrorism, or very serious crime, they are required to produce the Data Protection Act release form quoting either DPA Section 28 or 29 whichever is

applicable. However the Trust must still assure itself that the request is reasonable or it may not be indemnified against being prosecuted for a breach of confidentiality by the data subject(s).

- Any other subject access requests made under the provision of the Data Protection Act 1998 will be dealt with in accordance with the Act and the best practice guidance of the National CCTV User Group on release of data to third parties. A copy of the relevant data will be produced and sent out to the individual if all conditions of the Act are met. Viewing of such images will take place outside the CCTV Control Room.

13.4 **Prosecuting Authorities**

- Access to recorded material may be permitted to allow statutory prosecuting authorities, such as the Crown Prosecutor, the Customs and Excise, or the Health and Safety Executive, to investigate and prosecute serious breaches of the law.
- Prior authority of the Portering Security Manager/LSMS will be required and full details of the reason for granting access and the areas to be observed will be recorded in the Control Room Visitor log.
- The Portering Security Manager/LSMS must request the DPA 28/29 form prior to granting access when the request is in relation to 13.3 bullet 2.
- Images taken from a working copy of a DVD shall be placed in a sealed and completed evidence bag prior to its removal from the CCTV Control Room and the prosecuting authority shall be required to sign a disclaimer form accepting responsibility for the DVD in all respects. Relevant MG 11 form must be completed for all evidence handed over.

13.5 **Release of Recorded Material to the Media**

- The Police will be permitted to release recorded material to the media in connection with the investigation or detection of a crime. Prior approval of the Trust is not necessary before it is released to the press, but the material should only be released in strict compliance with the recommendations of the ACPO Media Advisory Group and Essex Police procedures.
- The Portering Security Manager/LSMS and Head of Communications should be advised of the release of the recorded material to the media and every effort should be made to give the notification prior to its release.
- Notwithstanding the recommendations of the Association of Chief Police Officers (ACPO), the Police must ensure that any recorded material which is released to the media is limited to that required to convey information relating only to the particular incident and that they shall ensure that material is issued with strict copyright conditions that do not allow it to be used for entertainment or any other purposes.

13.6 **Evidential Material**

- Recordings which are required for evidential purposes shall be treated as exhibits and shall be retained and stored in accordance with Procedures agreed with the Police and the Crown Prosecuting Services.
- Recorded images removed as evidential material must be contained within a sealed evidence bag and a completed disclaimer prior to their release. Continuity of evidence from that point resides with the Statutory Prosecuting Agency.

13.7 **Unused Evidential Material**

- All recorded material which has been viewed by an investigating or disclosure officer of a statutory prosecuting agency under the definition of a criminal investigation under CPIA 1996 part 2 section 23 (1) is either classified as evidential material or potential or unused material.
- In accordance with local Police policy, a working copy recording of all material viewed by an investigating officer, and deemed as potential unused material is to be made by the

officer, of relevant sections of the material with best practice of 15 minutes either side of the incident being permitted.

13.8 **Photographs, Still Prints and Other Information**

- Still prints shall not be taken as a matter of routine or without justifiable reasons.
- Still prints of live incidents shall only be taken where they are deemed to be essential by the Portering Security Manager/LSMS or at the request of the police officer/official in charge at the scene of an incident. The name of the person making the request should be recorded together with the time and date of the request in the request logbook. Still prints shall be considered as recorded material and all the procedures, restrictions and controls relating to taped material detailed in this Code shall apply.
- Photographs shall not be displayed and shall be kept in a binder or album and securely stored within the CCTV Control Centre at all times. Access to the photographs or still prints will be forbidden to anyone except CCTV operators, approved Trust staff or CCTV Independent Inspectors.
- Photographs or still prints received from statutory prosecuting agencies may be permitted within the CCTV Control Room for crime prevention, crime detection and apprehension purposes only, as permitted under the Crime and Disorder Act 1998. All such prints shall be stored in a separate binder and only with the express permission of the Portering Security Manager/LSMS. The prosecuting agency shall be responsible for the provision of up to date photographs and still prints together with their auditing and disposal, in accordance with the provision of evidence requirements.
- The Portering Security Manager/LSMS shall maintain procedures for the regular auditing of photographs and still prints by the prosecuting agency and shall refuse any such material, which relates to matters outside of the jurisdiction of this code.
- Any other personal data or information received from statutory prosecuting agencies will be subject to the same guidelines outlined above for still prints or photographs and shall be subject to the requirements of the Data Protection Act 1998.

13.9 **Retention, Editing and Deletion**

- Editing of original recorded material is not permitted. Editing of material copied onto a copy DVD may be permitted under the requirements of the Data Protection Act 1998 to preserve the identity of other individuals contained on a tape if an individual subject access enquiry is made under the Act.

- The Trust must comply with ICO Code of Practice which is reflected in the Trust's Retention and Destruction Schedule and CCTV images retained for a minimum of 31 days and then erased permanently.

- CCTV data will be kept for 31 days across the Trust.

14. Training

14.1 All security officers operating the CCTV system shall be appropriately trained to Security Industry Authority (SIA) standard.

14.2 All operators of CCTV equipment shall be trained in their responsibilities in accordance with the Trust's CCTV policy and Code of Practice.

14.3 All staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

14.4 Staff will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation. Training by camera installers will also be provided as appropriate.

14.5 Recorded material may on occasions be used for training and demonstration purposes but the material will be selected by the LSMS and its use will be strictly controlled.

15. Communication & Implementation

15.1 All staff will be made aware of the location of security related policies at Corporate Induction.

15.2 This policy will be available for all staff to access on the intranet and all staff have a duty to ensure they are aware of the content and adhere to the principles therein.

15.3 All directorates are required to disseminate this policy to their staff via local risk management committees.

16. Monitoring

16.1 The audit tool seen in Appendix 1 identifies the policy key performance indicators. An annual audit will be undertaken by the LSMS and will be conducted across all Trust premises where CCTV is in use.

16.2 The audit results will be presented to the Health and Safety group as part of the Security Report.

16.3 Any incidents in respect of this policy and all associated changes in practice will also be presented to the Health and Safety group as part of the Security Report.

17. Equality and Diversity

17.1 The Trust is committed to the provision of a service that is fair, accessible and meets the needs of all individuals.

18. References

- Data Protection Act 1998
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- CCTV Code of Practice
- Caldicott Report 1997
- Records Retention Schedule 2014
- ICO Code of Practice

CCTV POLICY AUDIT TOOL

DIRECTORATE/ DEPARTMENT:		DATE OF AUDIT :			
		YES	NO	N/A	COMMENTS
1.	Is access to the CCTV control room restricted to all but authorised personnel?				
3.	Is the CCTV Control Room Key Register completed when access is requested to the CCTV control room?				
4.	Are the correct procedures followed for persons requesting to view and/or record CCTV images?				
4.	Is the CCTV Control Room Access Register completed when persons request to view and/or record CCTV images?				
6.	Is all CCTV footage disposed of appropriately?				
7.	Are all cameras situated so they can only monitor the intended area of coverage and not positioned anywhere that would be considered private e.g. office or toilet?				
8.	Are signs in place showing that CCTV systems are in operation?				
9.	Have cameras been positioned to avoid capturing the images of persons not visiting the premises?				
10.	Is a procedure in place for operational equipment to be checked regularly and maintained to ensure it is in good working order?				
11.	Has a review of incidents involving CCTV systems been reviewed and analyses to identify trends and high risk incidents?				

Appendix 2

CCTV CONTROL ROOM KEY REGISTER

Date	Print Name	Signature	Organisation	Time Out	Time In	Reason for Entry into CCTV Room	Comments

Appendix 3

CCTV CONTROL ROOM ACCESS REGISTER

Date	Print Name	Reason for Entry into CCTV	Name of people (including organisation) who have viewed footage	Details of any images removed	Reason for Removal of Images	Evidence Bag Reference Number	Crime Reference Number	Details of Outcome of Following Review CCTV	Comments