Somerset Partnership NHS
NHS Foundation Trust

CLOSE CIRCUIT TELEVISION

(CCTV) POLICY

Version:	1
Ratified by:	Senior Mangers Operational Group
Date Ratified:	December 2013
Title of Originator/Author:	Head of Corporate Business
Title of Responsible Committee/Group:	Regulation Governance Group
Date issued:	January 2014
Review date:	November 2016 **extended to May 2017**
Relevant Staff Group/s:	All Trust staff involved with CCTV and other agencies as identified.

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

CONTENTS

DOCUMENT CONTROL

Reference AS/Oct13/CCTVP	**Version** 0.2	**Status** Final	**Author(s)** Head of Corporate Business
Amendments	This revised document reflects recent legislative changes in CCTV practice. Section 9 of the policy enables the Trust, using the appropriate safeguards, to record internal CCTV images within its mental health inpatient wards. The policy complies fully with the Home Office Surveillance Camera Code of Practice and NHS Protect Circular S/G/15/2013-14.		
Document objectives: The aim of this policy is to identify and implement responsible CCTV practices and procedures in order to supplement the overall protection of patients, staff and visitors.			
Intended recipients: All Trust staff and members of partner agencies.			
Committee/Group Consulted: Senior Managers' Operational Group, Executive Management Team			
Monitoring arrangements and indicators: Monitored through the Regulation Governance Committee			
Training/resource implications: As specified in Plan.			
Approving Body and date	Regulation Governance Group	Date: December 2013	
Formal Impact Assessment	Impact Part 1	Date: October 2013	
Ratification Body and date	Senior Managers' Operational Group	Date: December 2013	
Date of issue	January 2014		
Review date	November 2016 **extended to May 2017**		
Contact for review	Head of Corporate Business		
Lead Director	Director of Governance and Corporate Development		

CONTRIBUTION LIST Key individuals involved in developing the document

Name	**Designation or Group**
Andrew Sinclair	Head of Corporate Business/Equality and Diversity Lead
Phil Brice	Director of Governance and Corporate Development
Jean Glanville	Claims and Litigation Manager
Tracey Edwards	Local Security Management Specialist (LSMS)
Laurence Perrett	Information Governance Manager
Nick Woodhead	Legal Strategies Manager
Members	MH Ward Managers Group
Group Members	Senior Operational Managers' Group

1. INTRODUCTION

1.1 Somerset Partnership NHS Foundation Trust is committed to providing effective and efficient healthcare services. The Trust believes with the appropriate use of CCTV there is potential for both a reduction in crime and the promotion of health. In certain clinical situations the use of CCTV may assist in supervision of areas of the building and CCTV may also be beneficial to the healthcare of individuals who use the Trust's services.

1.2 The Trust acknowledges its responsibilities to protect staff, visitors and patients whilst on Trust property while also protecting the freedom of all individuals within the standards of the Human Rights Act, Data Protection Act 1998, Mental Health Act Guidance and other guidance which may be issued by the Information Commissioner and/or others from time to time.

1.3 The principal aim of this policy is to identify and implement responsible CCTV practices and procedures in order to supplement the overall protection of patients, staff and visitors. The Trust therefore acknowledges a specific responsibility to consider the implications of the use of CCTV and to implement policies and practices that will provide a responsible approach to the use of CCTV equipment. As part of the Trust's commitment to the quality and safety of the environment, this policy has been prepared to enable the Trust to set targets by which continuous monitoring of the proposed systems can be measured.

1.4 As a measure of this commitment the Trust will:

- Comply with all relevant legislation pertaining to the use of CCTV;
- Establish a CCTV management system, which would comply with the above mentioned standards for such systems
- Maintain the CCTV management system, adopting best practice where possible and strive to continually improve the monitoring control processes, through monitoring and assessment;
- Educate and train employees to understand the reasons, benefits and legal implications of the use of CCTV installation.

2. PURPOSE AND SCOPE

2.1 The purpose of this document is to provide policy guidance for the management of CCTV systems to support the health, safety and welfare of all persons on its properties. It aims to establish the principles and procedures for the recognition of and response to the legalities of using CCTV systems within the Trust. It provides guidance for all employees and others who are involved in CCTV systems so they are better equipped to avoid or minimise the risks of illegal use of any systems installed or existing systems. It will also ensure any CCTV system is not abused or misused and that CCTV is correctly and efficiently installed and operated.

2.2 The policy aims to ensure:

- The use of CCTV adheres to the principles of the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and other relevant legislation;
- Any CCTV system is not abused or misused;
- CCTV is correctly and efficiently installed and operated;
- Patients, staff and visitors can be assured of the safeguards in place;
- Increase personal safety and reduce the fear of crime;
- Protect the Trust's buildings and their assets;
- Support the Police and LSMS in a bid to deter and detect crime;
- Assist in identifying, apprehending and prosecuting offenders;
- Protect members of the public (including employees) and private property.

2.3 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 Trust premises. It also applies to anyone involved in the setup, use and management of CCTV cameras and is intended to cover all activities of the Trust and the areas where Trust activities are carried out, including those properties not owned but used by the Trust where the Trust have fitted cameras. The policy applies to all users of CCTV who monitor and record images from those areas to which the public have largely unrestricted access, under schemes used for the general purpose of crime prevention and public safety. It also applies to users of CCTV who in exceptional circumstances wish to carry out covert monitoring of spaces to which the public (including employees) has access.

3. OBJECTIVES

3.1 CCTV systems are registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will comply with the requirements of the Data Protection Act and the Information Commissioner's Code of Practice.

3.2 All associated information, documents and recordings obtained and used by CCTV is protected by the Data Protection Act.

3.3 Cameras will monitor activities on Trust premises and car parks to identify criminal activity whether occurring, anticipated, or perceived, and aim to enhance the safety and well-being of staff, patients and visitors.

3.4 Users are aware static cameras must not be permitted to focus on private homes, gardens or other areas of private property.

3.5 Except when specifically authorised by the Police using specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA), staff must not direct cameras at an individual, their property, or a specific group of individuals. Only the Police and NHS Protect are permitted to authorise Direct Surveillance, and this will be in relation to Trust sites only.

3.6 Images obtained from the use of CCTV will not be used for any commercial purpose. Recordings will only be released for use in investigation of a specific crime. Recordings will not be released to the media for purposes of entertainment.

3.7 The planning and design of the CCTV systems will endeavour to ensure maximum effectiveness and efficiency but cannot guarantee to cover or detect every incident occurring within the areas covered.

3.8 Warning signs, as required by the CCTV Code of Practice of the Information Commissioner and will be displayed at all access routes to areas covered by the Trust CCTV.

4. LEGAL FRAMEWORK AND REQUIREMENTS

4.1 Article 8 of the Human Rights Act 1998 protects the right to respect for private and family life. No Public Authority may interfere with this right except when in accordance with the law and when necessary. Any interference must be proportional to the threat or risk to community safety, comply with all relevant legal requirements, be necessary for safety and the prevention and detection of crime and cause the minimum of interference to the individual. The use of CCTV must therefore be open to scrutiny and be fully documented.

4.2 The Trust must be able to demonstrate that it complies with the Data Protection principles which state data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in accordance with individuals rights;
- Secure;
- Not transferred to countries without adequate protection.

4.3 The Information Commissioner has the power to issue Enforcement Notices where he/she considers there has been a breach of one or more of the Data Protection principles.

4.4 This policy should be read in conjunction with the Information Commissioner's *CCTV Code of Practice 2008* and the Home Office *Surveillance Camera Code of Practice June 2013*.

4.5 The Trust is required to comply with the guidelines within that document. This code provides good practice advice for those involved in operating CCTV and other devices which view or record images of individuals. It also covers other information derived from those images that relates to individuals.

4.6 The Regulation of Investigatory Powers Act 2000 and the Human Rights Act 1998 also need to be complied with in set circumstances. (please refer to Appendix A).

4.7 The Trust is also required to:

- Establish who is the person(s) or organisation(s) legally responsible for the proposed scheme;
- Assess the appropriateness of, and reasons for using CCTV or similar surveillance equipment (1st data protection principle);
- Document the assessment process and the reasons for the installation of the scheme;
- Establish the purpose of the scheme (1st & 2nd data protection principle);
- Ensure the notification by responsible Trust Director is lodged with the Office of the Information Commissioner covers the purpose for which this equipment is used;
- Establish and document the person(s) or organisation(s) responsible for ensuring the day-to-day compliance with the requirements of the Code of Practice;
- Establish and document security and disclosure policies.

5. DUTIES AND RESPONSIBILITIES

5.1 The **Chief Executive** has overall responsibility for ensuring CCTV use and data control are effectively addressed within the Trust.

5.2 The **Director of Governance and Corporate Development** is responsible for ensuring Trust compliance and will assume responsibility for the implementation of the CCTV Management System, ensuring:

- A CCTV Plan is prepared and reviewed annually by the Trust Board;
- CCTV issues feature in Trust Business Plans;
- Appropriate resources are made available for the installation and monitoring of CCTV installations that are designed to assist in the protection of staff, visitors and patients whilst on Trust properties.

The Director expressly authorises each CCTV installation, or an extension of an existing system, prior to use.

5.3 The **Local Security Management Service (LSMS)** will ensure effective management of installation use and monitoring issues within the Trust. The LSMS will ensure appropriate control measures are set and achieved and to ensure changes to Data Protection and Human Rights legislation are reflected within this policy. The LSMS will undertake an annual review of the CCTV policy. The review will include:

- How the CCTV installations and monitoring procedures should be adjusted to reflect changing conditions, information and legislation e.g. reflecting the outcomes of local managers' annual assessment of each

CCTV installation in operation. Such annual assessments will be copied to the LSMS (Local Security Management Specialist);

The LSMS in consultation with the Director and local CCTV managers will ensure that training on the use of CCTV is provided to members of staff who require such training, in line with this Policy.

5.4 **All Trust Staff** involved in the use of CCTV installations will receive training appropriate to their activities and responsibilities.

6. EXPLANATION OF TERMS USED

CCTV: Close Circuit Television which monitors and records images.

CCTV Manager: the person responsible for the site on which the CCTV is fitted.

Covert Surveillance: means surveillance, which is carried out in a manner to ensure the person subject to the surveillance is unaware that it is or may be taking place.

Data Protection Officer: the Trust's appointed Data Protection Officer.

Directed Surveillance: covert surveillance undertaken in relation to a specific investigation which is likely to result in the obtaining of private information about a person (whether specifically identified for the purpose of the investigation or not) otherwise than by way of an immediate response to events or circumstances.

Intrusive Surveillance: covert surveillance carried out in relation to anything taking place on premises (however temporary) or in any private vehicle. Police, Customs and security services, never NHS staff, should only carry out this type of surveillance.

Scheme/System: any of the Trust's CCTV schemes.

Trust: Somerset Partnership NHS Foundation Trust.

7. DESIGN CONSIDERATIONS

7.1 The installation of CCTV systems can significantly assist in the reduction of assaults and inappropriate access to and from the premises.

7.2 CCTV should not be regarded as a substitute for good sight lines being designed into a facility.

7.3 Internal CCTV systems should include the monitoring of areas such as patient corridors, day rooms, interview rooms, therapy rooms, vocational services, education spaces, visitors' room and reception lobbies.

7.4 External CCTV provisions should include the monitoring of secure perimeters, air-locks, vehicle access routes, car parking, pedestrian walkways, internal courtyards and main entrances to the building.

7.5 Consideration should be given to the best currently available technology but any CCTV system as a minimum should:

- Have the capability to record images 24 hours a day, 7 days a week;
- Retain images for determined period of time
- Be user-friendly;
- Easy to configure and adjust;
- Be capable of providing good night coverage.

7.6 CCTV systems, including remote monitoring and recording facilities, should meet the design, installation, functional, operational and performance requirements of BS EN 50132-5, BS EN 50132-7, BS 7958, BS 8418 and BS 8495.

7.7 CCTV cameras should be integrated into the main site CCTV system (with the exception of seclusion cameras), sited in accordance with the Trust's security strategy and supported by local procedures.

7.8 The design of the internal CCTV system should be carried out three-dimensionally taking into account the physical features of the area within which it is located. Rooms should also be designed to ensure that they are configured to maximise the views and minimise the numbers of the cameras required, and that configurations of installation are able to eliminate blind spots.

7.9 In addition, CCTV camera installations should be designed to:

- Produce high-quality digital images (colour images during the day);
- Be able to provide optimum viewing of the area required to be observed from each location;
- Be tamper-proof and non-ligature, minimise the opportunity for damage, and not be capable of being used as a climbing aid;
- Where possible, incorporate a housing that obscures the camera from view;
- Be operable under artificial lighting conditions, with or without natural lighting, avoiding the potential for flare due to nearby lamp intensities;
- Include stops to avoid any possibility of intrusive observation of adjacent private properties.

8. GENERAL APPROACH

8.1 The stages of the CCTV process described within this policy follow the "plan, implement, check and review" pathway. Where new systems are to be installed all four stages will be used. However, in existing installations only the "Check and Review" stages will be necessary. This will provide the framework for this Policy in support of the Information Governance requirements for data protection management requirements.

8.2 For the purposes of this guidance, Trust premises have been divided into three types of area:

Public Areas

8.3 These are areas of the premises to which the public have unrestricted access e.g. grounds, corridors, car parks etc. As elsewhere in Britain, CCTV is commonly in use in the public areas of Trust premises. There are no special considerations required beyond those placed by the Information Commissioner on all CCTV cameras, such as signage, notification etc. For instance, CCTV will be used to monitor people coming in and going out of the Trust to protect persons within the building and to assist in the prevention of unwelcome visitors**.**

Communal Areas

8.4 These are shared parts of premises i.e. by staff, patients, etc. They include dayrooms, dining areas, corridors. CCTV may be used in communal patient areas where the safety of either patients or the public is believed to justify this. It is central to any decision that, in line with the requirements of the Information Commissioner, a clear reason for installation is available.

Private Areas

8.5 These are those areas where any individual might reasonably expect privacy. These include bathrooms, bedrooms, toilets and seclusion rooms. The legal basis for using CCTV in private spaces arises either from an individual's capacity to consent or because such monitoring is an agreed and appropriate part of compulsory treatment (for patients detained under the Mental Health Act 1983) and is proportionate in an individual case. This means that while it may be legal to use cameras in bedrooms, seclusion rooms and toilets, there would be a considerable burden on the Trust to prove the intrusion was proportionate. It is also arguable the burden would be higher still if the cameras were linked to a recording device, rather than providing real-time unrecorded images.

8.6 The General Medical Council has provided guidance on making and using visual and audio recordings of patients, which sets out information about consent requirements. Very great care needs to be taken in the siting of monitors to ensure that there is no inappropriate deliberate or accidental viewing of images by unauthorised others. Further guidance about this is provided in the CCTV Code of Practice.

8.7 Particular consideration also needs to be given to issues of gender, and whether use of CCTV cameras in private areas provides any potential for increasing patient vulnerability, inappropriate behaviour, sexual harassment or abusive relationships.

8.8 **If the CCTV system is to operate within private areas in Trust premises then the following must be taken into account:**

- CCTV systems cannot replace clinical care and are by no means the answer to all security concerns; they can, nonetheless, offer a potential medium by which staff can enhance levels of care and security;

- The introduction of CCTV to private areas within inpatient wards should be given careful consideration, as it may not be in patients' best interests. The use of CCTV should be considered on an individual patient basis, based on risk and clinical assessments and discussions and decision make must be clearly recorded within the patient's healthcare record. Patients may consider CCTV intrusive and, in certain circumstances, it could have a negative effect on a patient's mental state;
- Article 8 of the European Convention on Human Rights affords 'the right to respect for private and family life'. It can, however, be interfered with by a public authority for the 'Protection of health';
- It is not uncommon for certain patient groups to be subject to regular monitoring that is consistent with their care plan but which clearly deprives them of an element of privacy. This may take the form of 'door openings or lights on and, in certain circumstances, CCTV, which may result in less interference with the patient from staff;
- If a decision is made to install CCTV within private areas of the inpatient areas, or new patients enter a ward, patients must be advised of the system and why it is being used. While a patient's consent is preferable, it is not required when the purpose of the system is considered to be in their best interests;
- Section 10 of the Data Protection Act 1998 gives those subject to CCTV the right to serve a written notice to a health body requesting such action ceases if it is alleged to be causing substantial unwarranted damage or distress to that individual or another person. If the purposed of the scheme is to protect the vital interests of the patient, the right to serve a notice does not apply. If such a notice is received, a reply must be given within 21 days, either indicating an intention to comply with it or giving an explanation as to why the notice is not justified. If such a request is granted, the camera should be either covered up or removed.

9. USE OF CCTV ON TRUST PREMISES

Initial Assessment Procedures

9.1 Before installing and using CCTV, it will be necessary to establish the purpose or purposes for which the equipment is going to be used and document the assessment process and the reasons for the local installation of equipment.

9.2 The local manager is legally responsible for the proposed scheme, local implementation, and day-to-day compliance with the requirements of the CCTV Code of Practice and MHA Guidance.

Positioning the Cameras

9.3 The equipment should be positioned in such a way that it only monitors those spaces which are intended to be covered by the equipment, based on the initial assessment and any subsequent review.

9.4 Ensure local managers and other staff users are aware of the purpose(s) for which the CCTV scheme has been established and they are only able to use

the equipment in order to achieve the purpose(s) for which it has been installed.

9.5 CCTV Signs complying with the requirements of the Safety Signs and Signals Regulations should be placed so that the staff, patients and public are aware they are entering, or are in an area which is covered by surveillance equipment. This signage should also include an image/picture of a camera as additional information. The signs should be clearly visible and legible and therefore the size of the signs may vary according to circumstances, e.g. a sign on entrance door to a building or in corridors may only need to be sized at A4 or A5 (at the smallest) because it is at eye level of those entering the premises.

9.6 Signs at entrances of sites and car parks alerting drivers/pedestrians to the fact the site and car parks are covered by such equipment will normally need to be large, for example A3 size as they are likely to be viewed from farther away.

9.7 All signs should state the Trust's name and set out the purpose of which the CCTV cameras are being used with a contact number of the contact person. The suggested wording is as follows: *Images are being monitored through CCTV for the purpose of (insert purpose) e.g. security of premises, public and employee safety, prevention of crime. This scheme is controlled by Somerset Partnership NHS Foundation Trust. For further information please contact (Name of Post) on (telephone number).*

Quality of the Images

9.8 It is important 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. Upon installation, an initial check should be undertaken to ensure the equipment performs properly.

Using CCTV systems

9.9 Operators of the CCTV will not target or track individuals arbitrarily or based on the nine protected characteristics as defined by the Equality Act 2010.

9.10 Security Cameras, monitors and recording equipment must be maintained in a working condition at all times. This is the responsibility of the local manager.

9.11 The location of each camera is documented on a map held by the Corporate Business Manager and Head of Division.

9.12 Any problems with cameras, monitors and recording equipment should be reported to the approved contractor for repair within 24 hours.

9.13 Any equipment failure must be noted in a fault repair log.

9.14 Should a camera, monitor or recording equipment fail to function it is the responsibility of the CCTV manager to satisfy him/herself that after repair the equipment is functioning properly.

9.15 At the start of every shift the Nurse-in-Charge must check:

- Digital Recordings are being made;
- The correct time and date are displayed on the recording system.

Processing and Retention of Images:-

9.16 Images should not be retained for longer than is necessary and not longer than 28 days.

9.17 Once the retention period has expired the images should be removed and erased.

9.18 If images are retained for evidential purposes, they should be retained in a secure place to which access is controlled and in a secure, locked storage system.

9.19 On removing the medium on which the images have been recorded for use in legal proceedings, this should be documented and a signature of the collecting officer obtained. Currently this should only be put on a CD-R/DVD-R as this is best evidence and the only one accepted in court hearings.

9.20 Monitors which display images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised staff.

9.21 Access to the recorded images should be restricted to designated members of staff. The Head of Division may authorise a viewing of a recording. Normally recordings will only be viewed if an incident has taken place. Records of viewings will be made on the control log.

9.22 The Head of Division is responsible for deciding whether to allow requests for access by third parties which should only be made in limited and prescribed circumstances, and only in consultation with the LSMS and the Trust Information Governance Officer.

9.23 Viewing of recorded images should take place in a restricted area and no unauthorised personnel should be allowed access when viewing is taking place. A report should be made to include the date, time, who was viewing, why, the outcome, if any, of the viewing and the date / time the images were removed if copied and taken to secure storage.

9.24 Any CDs required by the Police or other authorities for future evidential purposes shall be identified and passed to the LSMS or Corporate Business Manager to be properly secured and stored if not being held by the police. The Trust Data Protection Officer is also to be informed.

9.25 All recordings released to the police must be signed out in the control log. The following details will be recorded:

- Number of CD's with date and time span of recording:
- Name, Number, Police Station, relevant police department and phone number:
- Signature of person handing over recording.

9.26 Should the recording be returned without it being needed by the police again within the normal holding period it will be placed into storage until it is disposed of safely and securely.

Storage of Images

9.27 The storage system containing recorded images, recorded hard drives, compact disk (CD) etc. must be locked and access strictly limited to designated members of staff only.

10. INFORMATION

10.1 When a decision is made to install CCTV into communal patient areas, and whenever new patients enter the ward, patients should be advised of the system and the reasons for its use. Whilst a patient's consent to its use is preferable, it is not required when the purpose of the system is believed to be in the best interests of the patient or others on the ward.

10.2 All mental health patients should be given a leaflet explaining the Trust's policy on the use of CCTV cameras. This is not a requirement of the Data Protection Act, but is considered to be good practice in the context of care. The patient's understanding of the matter should be recorded along the lines similar to those used for informing detained patients of their rights under the Mental Health Act:

- The staff member briefing the patient about the use of CCTV should sign that [and when] they had done so;
- The staff member should provide a written assessment of the patient's understanding of the system;
- Where a patient does not understand, a date should be recorded for the next attempt to explain the practice;
- Information should be provided in the leaflet about the uses to which information from images may be put (including unexpected information, for example what would happen if any recording were made of criminal activity).

11. ACCESS TO DISCLOSE IMAGES TO THIRD PARTIES

11.1 Duty of Confidence – General

Information disclosed by an individual to a health care professional in the course of his or her work is covered by a duty of confidence. Consequently, patients' information held by the Trust is covered by this duty.

The data subject can request a copy of their record images under the principles of the Data Protection Act but it will only be provided if its production does not involve disproportionate effort. In all cases where a copy of a recording is requested by the data subject the advice of the Trust's LSMS and the Trust's Information Governance Officer must be taken on whether a copy of the recording should be provided.

11.2 Duty of Confidence – Disclosure to the Police

Under the duty of confidence, a patient's information may only be disclosed to third parties in the following circumstances:-

- The patient has given their informed and explicit consent in writing i.e. the patient must understand to whom the proposed disclosure will be made, the reason for the disclosure and the potential consequences of disclosure.
- It is a matter of judgment but in circumstances in which disclosure might be lawful include where disclosure is necessary for the detention or prevention of a crime or where disclosure is necessary to prevent serious harm coming to an individual. This will be done with a Data Protection Act.
- Where a court has ordered the information should be disclosed. On receipt of a court document that appears to require disclosure of information without the consent of the patient, staff should liaise with the LSMS and Information Governance Officer to ensure that all the relevant formalities have been complied with prior to disclosure of the information.

11.3 **Where statute requires disclosure of the information.**

In all cases and in liaison with the LSMS and Information Governance Officer disclosure to a third party should be limited to the minimum information required to satisfy the purposes of disclosure. Patient information should be anonymised whenever this would be sufficient for a particular purpose.

11.4 **Where images may be used as evidence in litigation against the Trust**

Where the image is requested in contemplation of a claim against the Trust to be used as evidence, the Claims and Litigation Manager at Mallard Court must be informed prior to the image being disclosed.

11.5 **Freedom of information**

The Trust may receive requests under the Freedom of Information Act 2000 (FOIA). The FOI Officer (Mallard Court) is responsible for responding to freedom of information requests and will respond within the required 20 working days as described within the FOI Policy.

11.6 Section 40 of the FOIA contains an exemption relating to information about individuals. If you receive a request for CCTV footage, we will consider:

- Are the images those of the requester? If so then that information is exempt from the FOIA. Instead this request should be treated as a data protection subject access.
- Are the images of other people? These can be disclosed only if disclosing the information in question does not breach the data protection principles.

11.7 In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to a FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA). This is not an exhaustive guide to handling FOI requests.

12. BREACHES OF POLICY

12.1 The Trust reserves the right to take action against any employee who breaches this policy in accordance with the Trust's employee relations procedures.

12.2 As a major purpose of these systems is in assisting to safeguard the health and safety of staff, patients and visitors, it should be noted intentional or reckless interference with any part of any monitoring equipment, including camera/monitors/back-up media, may be a criminal offence and will be regarded as a serious breach of Trust policy.

12.3 Where it is identified that there has been a breach of this Policy, or improper or misuse of the CCTV recording equipment, hardware or recorded images, then this should be reported to the Head of Division and LSMS.

13. COVERT SURVEILLANCE/TARGETED OBSERVATIONS

13.1 Only for specifically defined instances and in accordance with the declared purpose and objectives of these schemes, may such surveillance equipment be used for targeted observation. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates the use of covert / directed surveillance of the type and is subject to a strict Code of Practice set out below. Use of CCTV in these instances or for any other reason other than authorised in accordance with this policy is not permissible at any time or circumstance.

13.2 Covert Surveillance must be directed and undertaken for a specific investigation. Prior to any surveillance RIPA authorisation must be obtained. It must be proportionate to what it seeks to achieve, be necessary and have consideration to collateral intrusion. Managers and Directors may not be notified until after the investigation is complete depending on the circumstances

13.3 Authorisation can only be given:

- To prevent and detect crime;
- In the interests of Public Safety;
- For the purpose of Protecting Public Health.

13.4 The Police or Authorised Officers at NHS Protect are the only persons able to give authorisation and it must be obtained in every circumstance. They are not able to delegate this power.

13.5 Authorisation must be given in writing and will be valid for 3 months. It can be given orally only in urgent cases and this is only valid for 72 hours. No authorised officer is allowed to authorise his or her own activities. Appendix B shows the form, which has to be completed to request RIPA authorisation and this should be done in conjunction with the LSMS.

14. EQUALITY IMPACT ASSESSMENT

14.1 All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected

characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

15. TRAINING

15.1 Training takes place within the context of a training needs analysis undertaken by the Trust. A training strategy has been put in place to ensure staff are confident in their roles. The strategy includes the mechanism to identify, select and train staff:

- Understand the role they are to fulfil in the event of an incident;
- Have the necessary competences to fulfil that role;
- Have received training to fulfil these competencies.

16. MONITORING COMPLIANCE AND EFFECTIVENESS

16.1 Process for Monitoring Compliance

Overall monitoring will be by the Regulation Governance Group.

The Director of Governance and Corporate Development will be responsible for monitoring the effectiveness of the policy and for escalating concerns or risk issues to the Executive Management Team.

The Regulation Governance Group will receive quarterly reports from the Health, Safety and Security Management Group who will identify recent incidents and areas of concern.

16.2 Methodology to be used for monitoring

- Incident reporting and monitoring;
- Risk assessment and emergency planning risk register.

A brief of the any lessons learnt will be provided to staff to raise awareness through the 'what'son@sompar' Trustwide newsletter.

17. RELEVANT CARE QUALITY COMMISSION (CQC) REGISTRATION STANDARDS

17.1 The standards and outcomes which inform this procedural document, are as follows:

Section	Outcome	
Information and involvement	1	Respecting and involving people who use services
	2	Consent to care and treatment
Personalised care, treatment and support	4	Care and welfare of people who use services

Safeguarding and safety	7	Safeguarding people who use services from abuse
	10	Safety and suitability of premises
	11	Safety, availability and suitability of equipment
Suitability of staffing	14	Supporting workers
Quality and management		
	20	Notification of other incidents
	21	Records

18. COUNTER FRAUD

18.1 The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

19. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

19.1 National Documents

The Home Office Surveillance Camera Code of Practice June 2013 is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

The CCTV Code of Practice and more information about the Data Protection Act is available from the Information Commissioner's Office by telephoning 01625 545 745, or at www.informationcommissioner.gov.uk

The Care Quality Commission (CQC)

http://www.cqc.org.uk/

The General Medical Council issued guidance in 2002 on Making and Using Visual and Audio Recordings of Patients. This is available at www.gmcuk.org/standards/aud_vid.htm

Health Building Note 03-01: Adult acute mental health units (Department of Health)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/147864/HBN_03-01_Final.pdf

19.2 Other Useful websites:

www.cctvusergroup.com

The National CCTV User Group

www.crimereduction.gov.uk/toolkits

The Governments crime reduction toolkit

www.homeoffice.gov.uk

http://hosdb.homeoffice.gov.uk/publication/docs/or manual.pdf

CCTV Operational Requirements Manual

www.nahs.org.uk

National Association for Healthcare Security

www.securedbydesign.com/pdfs/SBD Hospitals 110405.pdf

Secured by Design for Hospitals

www.the-sia.org.uk

The Security Industry Authority – training and licensing of people employed in the security Industry.

19.3 References

Data Protection Act 1998

Information Commissioners Codes of Practice

Mental Health Act Code of Practice

Regulation of Investigatory Powers Act 2000

Human Rights Act 1998

Data Protection Commissioner Codes of Practice

Private and Voluntary Health Care Regulations 2001

19.4 Cross reference to other procedural documents

This Closed Circuit Television (CCTV) Policy should be read in conjunction with the following related Trust policies:

Confidentiality and Data Protection Policy;

Freedom of Information Policy;

IM&T Security Policy;

Information Governance Policy;

Records Keeping and Records Management Policy;

Risk Management Policy and Procedure;

Security Policy;

Untoward Event Reporting Policy and procedure

All current policies and procedures are accessible to all staff on the Trust intranet (on the home page, click on 'Policies and Procedures'). Trust Guidance is accessible to staff on the Trust Intranet (within Policies and Procedures).

20. APPENDICES

For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.

Appendix A	Application for Access to Recorded Images by Data Subjects
Appendix B	Simple Guide for LSMSs and Managers to ensure Lawful and Best Practice for using CCTVs On Inpatient Environments
Appendix C	CCTV New Installation or Annual Review Checklist
Appendix D	Part Ii of The Regulation of Investigatory Powers Act (Ripa) 2000 Authorisation Directed Surveillance
Appendix E	CCTV Register Form
Appendix F	Local CCTV Procedure

APPENDIX A

APPLICATION FOR ACCESS TO RECORDED IMAGES BY DATA SUBJECTS

The Trust will only accept applications from the data subject, not persons acting on their behalf, except in a case where an application is made on behalf of a child under 16 years of age by someone with parental responsibility for the child or an application is made on someone's behalf by a legal representative but only if the express consent of the data subject accompanies the request.

APPLICATION DETAILS

Name of Applicant……..……
Address ……
……..……**Post Code** ……..……..
Name of Data Subject
…….
(If different from name of applicant)

Please provide details of the date, time and location of when you believe you may have been recorded. If you wish to make an application to see any other occasions where you may have been recorded, please attach a separate form with the details. Only one search fee (see below) is payable if the application forms are received at the same time.

Location …….
Vehicle Registration Number:……..…
Only complete if you believe that your image was captured whilst you were travelling in a vehicle.

Date ……..…….. **Time** ……..……..……
Please state a time span or a specific time am or pm

Proof of the applicant's identity (i.e. passport or driving licence) will be required before access to or disclosure of recorded material is permitted. In the case of applications made on behalf of children, the child's consent may also be required. You will receive a written response to your application within 21 days. In line with the Data Protection Act access to recorded images will be provided within 40 days of receiving the required fee and information.

1. I wish only to view the recorded image(s) YES/NO*
2. I enclose recent colour photographs of myself/the applicant in order that you can locate the correct image YES/NA*
Two colour photo booth style photographs must be provided, one of which is full face and the other a side on perspective.
3. I enclose a £10 cheque, made payable to Somerset Partnership NHS Foundation Trust, in payment for the search to be completed.

I authorise the deduction of £10 from my hospital account in payment for the search to be completed*
Signed ……..…… **Date** ……..…
Delete as appropriate

APPENDIX B

SIMPLE GUIDE FOR LSMSs AND MANAGERS TO ENSURE LAWFUL AND BEST PRACTICE FOR USING CCTVs ON INPATIENT ENVIRONMENTS

When inspectors or commissioners are visiting inpatient wards and hospitals units where CCTV has been installed, they may wish to consider the list of questions below in order to assure themselves that CCTV (or other surveillance equipment) is being used in a manner appropriate to this particular setting and which affords protection of human rights. This document is thus intended as a framework to enable an appropriate assessment to be made in a consistent manner.

	Question	**Regulatory source**
1.	Is the code of practice on CCTV issued by the Office of the Information Commissioner being adhered to? (You might want to consider both whether this was used as a guide for the original installation and whether it is still being applied rigorously).	Code of Practice on CCTV 2008
2.	What was the objective of installing CCTV?	Code of Practice on CCTV 2008
3.	Is there any evidence that CCTV is being used to compensate for a lack of adequate staffing levels?	Good Practice
4.	Was the installation of CCTV a proportionate response to the identified need?	Human Rights Act (article 8)
5.	Have the objectives of the installation been met? (And has any review or evaluation been undertaken to provide evidence to show this?)	Code of Practice on CCTV 2008
6.	Who within the organisation has overall responsibility for information governance, including the use of CCTV? Who has day-to-day responsibility for the use of CCTV (for example, at ward level)? Is this issue regularly considered at Board level?	Code of Practice on CCTV 2008
7.	What arrangements are in place to ensure that staff understand and receive training in the purpose and use of CCTV? Which staff are these (at what level)?	Code of Practice on CCTV 2008
8.	Is there a formal system in place for raising concerns or making a complaint about the use of CCTV and is this advertised clearly?	Code of Practice on CCTV 2008
9.	What was the process of decision-making which led to the installation of CCTV? What kind of patient consultation took place?	Good Practice
10.	Is there a process in place to ensure that the continuing use of CCTV is reviewed and that patients are consulted on this?	Good Practice
11.	What arrangements are in place to ensure patients Good Practice understand the purpose of CCTV and have access to the policies governing installation and use? (For example, is there a readily accessible patient	(Possibly Section 132 of the Mental Health Act for detained patients)

	leaflet? Is there a proactive approach to informing patients, having regard to their mental state, on admission and at other times?)	
12.	What arrangements are in place to ensure patients have access to any stored media which include images of themselves?	Code of Practice on CCTV 2008
13.	In the event of a request for access to the images by outside agencies such as the police, what process is in place to assess and authorise the request? Who is the named person responsible for this?	Code of Practice on CCTV 2008
14.	In the event a patient requests access to images of him/herself, what arrangements are in place to ensure that third party confidentiality is not breached?	Code of Practice on CCTV 2008
15.	What arrangements are in place for the disposal of recorded material after expiry of the permitted period of retention?	Code of Practice on CCTV 2008
16.	What processes are in place to assess the need for and decide on the implementation of changes in camera coverage?	Good Practice/ RIPA 2000
17.	For uses which require explicit informed consent (for example, for filming as part of treatment or in normally private areas such as bedrooms), what is the process for providing information to the individual about the process and for obtaining his or her consent?	Human Rights Act – Article 8 GMC guidance on the making and use of audio and visual recordings of patients (part 3)
18.	Does the policy allow for any use of covert CCTV? If so, is it in line with legislative requirements?	Regulation of Investigatory Powers Act 2000

APPENDIX C

CCTV NEW INSTALLATION OR ANNUAL REVIEW CHECKLIST

1. Why is the installation required?

2. Who has authorised the installation /continuation?

3. Who locally/which local post holder will oversee the installation/operation of the system?

4. Is there a local plan showing the cameras positions?

5. How many cameras are there?

6. Are the cameras fixed?

7. Are the cameras tilt /pan and zoom?

8. Are the cameras black and white, colour or day/night cameras ?

9. Are the cameras in public/communal or private areas? [Refer to policy]

10. Are images recorded or monitored?

11. If the images are monitored - by whom?

12. What format are the images recorded then onto hard drive?

13. Are images kept for up to 31 days then recorded over

14. Are the recorders and recordings kept locked?

15. Is access to the recorders /recordings controlled?

16. Is training available – is it recorded?

17. Are records kept of staff authorised to access the system including who may have access to recordings?

19. Is signage displayed informing the use of CCTV?

APPENDIX D

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000
AUTHORISATION DIRECTED SURVEILLANCE

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]
2. Describe the purpose of the specific operation or investigation.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4. The identities, where known, of those to be subject of the directed surveillance.
• Name: • Address: • DOB: • Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*
• In the interests of national security; • For the purpose of preventing or detecting crime or of preventing disorder; • In the interests of the economic well-being of the United Kingdom; • In the interests of public safety; • for the purpose of protecting public health; • for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].
8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **1.1 Describe precautions you will take to minimise collateral intrusion.**
9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?
10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		1.2 Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].**
14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

1.3 Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		**Grade / Rank**	
Signature		**Date and time**	
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]			

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.				
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.				
Name (Print)		**Grade/ Rank**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorities – check Code of Practice	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June			

APPENDIX E

CCTV REGISTER FORM

There are … CCTV cameras monitored at Somerset Partnership NHS Foundation Trust. In addition, … cameras are monitored by individual Departments/Wards and are used in conjunction with Door Access Systems … cameras are monitored from within the Security Control for the purpose of prevention and detection of crime and for staff, patient, and visitor safety

Types of Cameras	**Numbers**
Pan, Tilt, Zoom (PTZ)	
Dome	
Static	
Covert	
Off-site cameras	

	Camera Position	**Type**	**Monitored By Security Control**	**Used in conjunction with Door Access**	**Owned By**
e.g.	**Ladysmith Building**	**Dome**	**Yes**		**Acute**
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					

APPENDIX F

LOCAL CCTV PROCEDURE

Location _____

This local procedure is to be read in conjunction with guidance taken from the Trust's CCTV policy.

The System in Use
(Location) _____has (number) cameras linked to a hard drive in a (location e.g. locked area of reception).

The cameras are fixed/pan/tilt, black and white/colour day/night installed to view the immediate
surrounding areas of _____ (Location).

Under no circumstances must the cameras be used/adjusted to view surrounding areas and/or non-Trust properties.

The hard drive records images that are retrievable for (state number of) days

The system is serviced by (Provider of service and telephone number) and a maintenance log of work carried out on CCTV equipment is securely held within the control room.

The Purpose of the System

State purpose e.g. the security of premises, public and employee safety and the prevention and detection of crime.

If existing system, state brief reasons why the system was originally installed e.g. a CCTV system has been in use for a number of years the reason for the installation was in response to a number of incidents that took place including theft of Trust property and to monitor unauthorised access to the building.

Location of Cameras
Attach a drawing showing the positions/number of cameras at the location indicating the direction of shot. Indicate the location of CCTV signs.

Control Measures
The local manager responsible for the system is (Name) (Designation) who will be responsible for the Day-to Day compliance with the Trust's CCTV policy.

Only those staff working with the CCTV system and the LSMS will have access to the CCTV control room.

All staff operating the CCTV system will receive training on its use. Records of training will be held in the control room information folder.

The manual for the system will be held in the ? information folder.
Any requests for data held on the system [viewing or copied] will be in conjunction with the Trust's CCTV policy i.e. the name and contact details of the requester will be held ? information folder also detailing date and time of request. No data may be released without the permission of those identified in the Trust's CCTV policy.

If data is released an entry will be made in the ? information folder detailing the data released, to whom, and time accompanied by a signature of the requester.

Signs detailing that CCTV is in operation will be placed as indicated.

Signs will comply with the requirements of the Trust policy.

Complaints received regarding CCTV usage will be passed onto the LSMS with a copy retained ? information folder.

Reviews

The local procedure will be reviewed on an annual basis and a copy of the reviewed procedure will be sent to the LSMS for information.

A weekly check will be made of the quality of images, action taken if not to standard and records held within the ? folder

Date _____