Policy for Surveillance Camera System

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	To provide guidance over the management of security and violence and aggression within the work place.
Document Type	[X] Policy [ ] SOP [ ] Guideline
Reference Number	Solent NHST/Policy/IG08
Version	Version 2
Name of Approving Committees/Groups	Policy Steering Group Assurance Committee
Operational Date	March 2017
Document Review Date	March 2020
Document Sponsors (Job Title)	Director of Finance
Document Manager (Job Title)	Local Security Management Specialist.
Document developed in consultation with	H&S Sub-Committee
Intranet Location	Business Zone / Policies, SOPs and Clinical Guidelines
Website Location	Publication Scheme / Policies and Procedures
Keywords (for website/intranet uploading)	Surveillance Camera System, Security

Policy for Surveillance Systems

Annex's

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1	01 Mar 16	Title	CCTV will now be known as Surveillance Camera System	01 Mar 16
2	25 Feb 2019	5 8	2.1 Scope wording update 8.4 updated signage wording	Feb 2019

Review Log

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
1				
2				
3				

Executive Summary

This revised policy gives comprehensive guidance to ensure the management of Surveillance Camera Systems is an essential part of ensuring the safety and security of staff and patients utilising Solent NHS Trust facilities.

Solent NHs Trust recognises their legal obligations under the references listed within Annex .

By the means of this policy and arrangements, Solent NHS Trust aims to ensure that no footage or images of staff, patients or visitors will be released or viewed by unauthorized person. That the system is regularly checked to certify that, if required, it is of an evidential quality to allow the Trust to pursue a prosecution.

1. INTRODUCTION & PURPOSE

1.1 Introduction

1.1.1 This policy aims to identify and support staff in the safe implementation and use of Surveillance Cameras in order to protect all staff, patients and public using Trust premises. The Trust acknowledges its responsibility to protect staff, patients and the public who use the services whilst on Trust property while protecting the freedom of all individuals within the standards of the Human Rights Act, Data Protection Act 1998, and other guidance which may be issued by the Information Commissioner.

1.1.2 As part of our commitment to ensure the delivery of high quality and safety working environment for our staff, patients and visitors who access our facilities, we will;

- Comply with relevant legislation pertaining to the use of surveillance cameras and recording equipment.
- Establish a surveillance camera management system.
- Maintain the surveillance camera system, adopting best practice where possible and strive to continually improve the monitoring control process through monitoring and assessments.
- Provide clear guidance to relevant staff to ensure they understand the reasons, benefits and legal implications of the use of surveillance camera.

1.2 Purpose

1.2.1 This policy will assist operators of surveillance camera systems in Solent NHS Trust to understand their legal obligations whilst also reassuring the public and patients using our services about the safeguards in place in relation to compliance with the Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Surveillance Camera Code of Practise 2013, The Surveillance Camera Code of Practice Information Commissioner 2014, The Caldicott Report 1997, Care Quality Commission Using Surveillance 2014 and other relevant legislation and guidance. It is anticipated that compliance with the this Policy & Procedure will ensure that;

- Surveillance Camera systems are not abused or misused
- Surveillance camera is correctly and appropriately installed and operated

1.2.2 Surveillance Camera will be used to help prevent and detect crime, including protection of Trust premises and to pursue the prosecution of offenders. In certain clinical situations the use of cameras is forbidden.

1.2.3 Surveillance Camera may assist in the robust monitoring of areas that may need observing to maintain levels of safety and security to those people utilising the Trusts facilities.

1.2.4 Surveillance cameras alone will not prevent staff or patients being assaulted or property from being stolen or damaged. However, combined with good local systems and procedures as part of a holistic solution, it can help to prevent and deter security-related incidents, as well as provide evidence to assist investigations of incidents.

2 SCOPE & DEFINITIONS

2.1 This policy applies to all bank, locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), Non-Executive Directors, and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.

2.2 Common abbreviations, definitions and terms used throughout this policy are provided in a glossary in Appendix 3.

3. ROLES & RESPONSIBILITIES

3.1 The Chief Executive is ultimately responsible for the manner in which the Trust implements the Surveillance Camera policy and adheres to agreed Data Protection requirements.

3.2 The Chief Nurse is Security Management Director (SMD) responsible for the overall management of the Trusts Surveillance Camera system and ensuring this policy and Codes of Practise issued by Information Commissioner (IC) are complied with.

3.3 Information Governance is responsible for providing advice to the Local Security Management Specialist (LSMS) and systems managers who are designated as the responsible persons on the disclosure of material in response to subject requests. They will also ensure the use of Surveillance Camera equipment on Trust premises has been registered with the Information Commissioner and the notification for the purpose is maintained.

3.4 Information Governance is responsible for ensuring that Surveillance Camera arrangements comply with the Data Protection Act principles which state that data must be;

- Fairly and lawfully processed.
- Processed for limited purpose and not in any manner incompatible with those purposes.
- Adequate, relevant and not excessive.
- Accurate
- Not kept any longer than necessary.

- Processed in accordance with individual rights.
- Secure at all times.
- Not transferred to locations without adequate protection.

3.5 The system managers and LSMS in liaison with Information Governance will ensure that;

- Appropriate access and reasons for using Surveillance Camera or similar surveillance equipment.
- Documentation of the assessment process and the reasons for installation.
- Ensure documentation the person(s) or organisation (s) responsible for ensuring the day-to-day compliance with requirements of the Code of Practise.
- Establishment and document security and disclosure policies and procedures for Surveillance Camera.

3.6 Local Security Management Specialist (LSMS) is responsible for providing advice on the provision of access and material to law enforcement agencies including Police, as well as advising on the provisions of the Surveillance Camera Code of Practise and the provision of new or additional Surveillance Camera equipment, in association with the Information Governance Manager.

3.7 Authorised Person (those staff trained) is responsible for the safe operating of Surveillance Camera equipment on behalf of the Trust whilst carrying out their daily duties. The authorised person will be provided with clear instructions and guidance on how to operate the equipment safely and proficiently. They must complete a daily Surveillance Camera log (produced locally) ensuring that the date and time are checked for accuracy, a check that the cameras are working and that the quality of the recorded image is checked. Any faults must be reported immediately, or at the next practicable time, to their line manager.

4. USING SURVEILLANCE CAMERAS

4.1 Management review using a Surveillance Camera system can be seen as intrusive. It is essential that due consideration is given to the need to maintain privacy and dignity at all times. It is important to remember that Surveillance Camera is not the sole answer to all security and monitoring needs. Due consideration of other means of keeping staff, patients, visitors and property safe should be undertake prior to settling on installing a new Surveillance Camera system.

4.2 Before installing a new Surveillance Camera system it will be necessary to establish the purpose of use for which the equipment is being purchased and installed.

4.3 Where people lack the mental capacity to understand, or consent, to the use of surveillance, clinical leads must make decisions in accordance with statutory principles of the Mental Capacity Act 2005.

5. LOCATION of SURVEILLANCE CAMERAS

5.1 There are three main areas of consideration when positioning Surveillance Camera;

(1) Public areas – These are areas around Trust property to which the public have unrestricted access e.g grounds, car park, main entrance etc. There should be valid reasons to position cameras at these locations such as staff and visitor safety and vehicle security but due consideration of the risk posed needs to take place.

(2) Communal Areas – These are shared areas on the Trust buildings foot print. They can include dayrooms, dining areas or corridors. Cameras can be placed in communal patient areas where safety of either people who use the services, staff or visitors justifies the positioning. It is central to any decision that, in line with the requirements of the ICO, a clear reason for installation is available. This could be in the form of a Risk Assessment highlighting incidence that have occurred within a specific area.

(3) Private Areas – Cameras should NEVER be installed within private areas such as toilets, bathrooms or shower rooms.

5.2 Prior to any surveillance cameras being fitted within seclusion rooms/136 suite, the Operations Manager of the relevant department, in liaison with the LSMS, is to seek legal advice in regards to the impact of cameras within these areas under Article 8 of the Human Rights Act 1998 and, complete a Privacy Impact Assessment form and submit it to the head of Information Governance for approval.

6. COVERT RECORDING

6.1 Covert recording utilising a Surveillance Camera system, or additional cameras, will not be undertaken without consultation with the Trusts SMD, Trust HR Manager, Trust Operation Manager Legal Services and always in accordance with the laws and legislation stipulated within the Regulation of Investigatory Powers Act 2000 (RIPA).

6.2 In accordance with the Human Rights Act 1998, Article 8 states that 'All persons have a right to a private life' and, under the Mental Health Act 1983, Section 8.4 states 'Hospital staff should make a conscious effort to respect the privacy and dignity of patients as far as possible while maintaining safety, including enabling a patient to wash and dress in private'.

7. POSITIONING of CAMERAS

7.1 Cameras should not be hidden from view but positioned in locations where they are secure and protected from vandalism. Where practicable, cameras must be capable of masking neighbouring spaces to prevent inadvertent visual intrusion.

7.2 Signs must be displayed informing staff, patients and visitors of the presence of a Surveillance Camera system.

7.3 Viewing monitors must be sited out of public/staff view, where the images can only be seen by authorised staff.

8. **SIGNAGE**

8.1 All signs should be placed so that the public are aware that they are entering a location covered by surveillance equipment. The signs must contain the following information;

- Identify the organisation responsible for the system i.e Solent NHS Trust.
- The purpose of the system.
- Details of whom to contact regarding the system (e.g Information Governance.)

8.2 The following wording is recommended on all signage;

These NHS premises are under CCTV Surveillance.
Images are being recorded and monitored for the Purposes
Of the prevention and detection of crime and for Public Safety

The scheme Is operated by Solent NHS Trust and for Subject Access Requests
Or Queries please contact the Data Controller Via email On
InformationGovernanceTeam@solent.nhs.uk
Or Call 0300 123 3919

Quoting Scheme ID: (add Hospital / Location)

9. **QUALITY of IMAGES**

9.1 It is vital for a system that the images produced are of a sufficient quality to enable the recognition and identification of persons suspected of committing acts of unlawful intention.

9.2 All systems must be installed and maintained by appropriately certificated contractors. Upon installation all equipment is to be tested to ensure that only designated areas are covered by the cameras and high quality images are available in live and play back modes. All Surveillance Camera equipment should be serviced annually and maintained when required.

10. **STORAGE & RETENTION of IMAGES**

10.1 All recordings, whether CDR, DVDR or hard disc, must be traceable. There are several elements to this:

- All recordings must be logged and traceable. For Digital Video Recorders (hard disc) systems, this means ensuring the system is set up to record with a date and time stamp.

- All incidents requiring provision of images must be logged within the daily occurrence book and a signature gained from the authorised person receiving the recording.

10.2 A daily Surveillance Camera log must be completed by an authorised person, the date and time of the system should be checked for accuracy and a check that all cameras are functioning correctly.

11. MANAGEMENT of HARD DISC SYSTEMS

11.1 Images must not be retained for any longer than necessary, normally 28 days. Each site that has Surveillance Camera in situ must adhere to the Information Commissioners Code of Practise and the Department of Health Code of Practise for Records Management which states that images can only be kept on a recording system for a maximum of 31 days. Once this time frame has expired the images must be erased. On most modern systems this will automatically be done.

12. DISCLOSURE of IMAGES TO THE MEDIA

12.1 The decision to release Surveillance Camera footage to the media in a non-Police situation can only be taken by the Chief Executive after consultation with the SMD/LSMS, Media Operations Team, Information Governance and NHS Protect.

12.2 If it is decided that images will be disclosed to the media, images of those persons not involved in the incident must be disguised or blurred so that identification is impossible. If the system does not have this facility than an editing company will need to be established that will perform this function.

13. ACCESS BY DATA SUBJECTS

13.1 The Data Protection Act provides Data Subjects (persons to whom 'personal data' relates) with the right to access data concerning them, including images obtained by Surveillance Camera.

13.2 Requests for Data Subject Access should be made on the appropriate application form (available from Information Governance) and submitted to the Trusts Information Security Manager.

13.3 Access and discloser to images is only permitted if it supports the purpose of an investigation. Under these conditions the request should be made through the LSMS or Information Governance Team. In a time critical situation authorised staff can issue a copy of Surveillance Camera footage to the Police or other Government agency. The request form would then be submitted retrospectively.

14. SURVEILLANCE FOOTAGE FOR DISCIPLINARY PURPOSES

14.1 Only in the event that Surveillance Camera footage shows activity that gives rise to concern may it be considered during the investigatory stages of a formal disciplinary procedure. It may only be used in formal disciplinary hearings when relevant to the allegations against the staff member and can be shown to prove, or disprove, the accusations.

14.2 Activity where Surveillance Camera can be provided to a Human Resource investigation may include;

- Acts which constitute Gross Misconduct in accordance with Trust policy.
- Practices that seriously jeopardise the health and safety of other staff, patients or visitors.
- Inappropriate treatment of patients.

14.3 In cases where Surveillance Camera footage is used in a disciplinary hearing, the accused will be given the opportunity to review the Surveillance Camera footage and explain, or challenge its content.

14.4 If the Trust identifies Surveillance Camera footage/images relevant to formal proceedings, then the timescale (28 days) for the retention of Surveillance Camera footage/images shall not apply. Footage/images retained for such purposes will be held for three (3) years following the completion of all disciplinary procedures, including any appeals process.

15. ACCESS, DISCLOSURE AND VIEWING OF SURVEILLANCE FOOTAGE BY THIRD PARTIES

15.1 Disclosure of recorded material will only be made to a third party in strict compliance with the Data Protection Act 1998 and any other relevant legislation, after authorised and served appropriate documentation is received by the Trusts LSMS or Information Governance Lead.

15.2 All access by Third Parties, and the medium on which it's recorded, must be documented on the relevant forms. Likewise, if access is refused this must also be documented.

15.3 Information on the documentation of issue must include:

- Date and time of request
- Description of incident
- Camera identifying incident
- Date and time on the image
- The reason why recorded medium was removed and/or crime/incident number
- Full details of person receiving the recording e.g Police number and home station
- Signature
- Date, location and method of destruction
- Details of person carrying out the destruction

16. VIEWING OF LIVE IMAGES

16.1 Viewing of live images must be restricted to operators only, unless specifically authorised by the LSMS or Information Governance Manager. (In the case of an emergency, Police/Government Agencies can view without specific authorisation.)

16.2 Surveillance Camera monitors must be positioned in a way that the general public, or unauthorised staff members, cannot view the images indiscreetly or inadvertently when passing.

17. REQUEST TO PREVENT PROCESSING

17.1 An individual has the right to request a Prevention of Processing where not doing so is likely to cause substantial and unwarranted damage to the individual.

17.2 All such requests should be addressed to the Information Governance Manager who must provide a written response within 20 days of the initial request, setting out their decision on the request and the reasons why.

18. DISPOSAL of DOCUMENTATION

18.1 All documentation relating to the management and operation of a Surveillance Camera system, together with all request forms must be retained by the system manager for a minimum of three (3) years after which destruction can only be authorised by the Information Governance Manager. All documentation must be disposed of as CONFIDENTIAL waste and be either incinerated or shredded by an authorised provider.

19. POLICY BREACHES

19.1 The Trust reserves the right to take disciplinary action, in line with the Trusts disciplinary procedures, against any employee who breaches this policy either deliberately, unintentionally or through carless neglect or actions.

19.2 The main purpose of a Surveillance Camera system is to assist the Trust in safeguarding staff, patients, and visitors and Trust property. Any deliberate disabling of Surveillance Camera system, reckless interference with any part of the equipment may be deemed as a criminal offence which would result in Trust/civil disciplinary being pursued.

20. REFERENCES

20.1 The following items of legislation are relevant to this policy;

- Criminal & Disorder Act 1998
- Criminal Justice & Public Order Act 1994
- Criminal Procedure & Investigation Act 1996
- Data Protection Act 1984
- Human Rights Act 1998
- Private Security Industry Act 2001
- Police & Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000

20.2 The following external publications have helped the development of this policy;

- NHS Protect Guidance on CCTV Systems
- Home Office CCTV Operational Requirement Manual 2009 (Publication 28/29)

Annex A

Equality Impact Assessment

Step 1 – Scoping; identify the policies aims	Answer
1. What are the main aims and objectives of the document?	To provide guidance to managers and staff over the management of all issues relating to security and violence and aggression.
2. Who will be affected by it?	All staff
3. What are the existing performance indicators/measures for this? What are the outcomes you want to achieve?	Reduction in loss, improved management of challenging behaviour, reduction in severity of incidents of aggression directed at staff.
4. What information do you already have on the equality impact of this document?	Existing incident report data.
5. Are there demographic changes or trends locally to be considered?	No
6. What other information do you need?	None

Step 2 - Assessing the Impact; consider the data and research	Yes	No	Answer (Evidence)
1. Could the document unlawfully against any group?		No	
2. Can any group benefit or be excluded?		No	
3. Can any group be denied fair & equal access to or treatment as a result of this document?		No	
4. Can this actively promote good relations with and between different groups?		No	
5. Have you carried out any consultation internally/externally with relevant individual groups?	Yes		
6. Have you used a variety of different methods of consultation/involvement		No	
Mental Capacity Act implications	Yes		
7. Will this document require a decision to be made by or about a service user? (Refer to the Mental Capacity Act document for further information)	Yes		In determining whether sanction is appropriate

If there is no negative impact – end the Impact Assessment here.

Step 3 - Recommendations and Action Plans	Answer
1. Is the impact low, medium or high?	
2. What action/modification needs to be taken to minimise or eliminate the negative impact?	
3. Are there likely to be different outcomes with any modifications? Explain these?	

Step 4- Implementation, Monitoring and Review	**Answer**
1. What are the implementation and monitoring arrangements, including timescales?	
2. Who within the Department/Team will be responsible for monitoring and regular review of the document?	

Step 5 - Publishing the Results	**Answer**
How will the results of this assessment be published and where? (It is essential that there is documented evidence of why decisions were made).	

****Retain a copy and also include as an appendix to the document**

Annex B

Application to Access Surveillance Camera Images

Applicants Details

Surname: …… Forenames: ……..

Company/Address: ……

Telephone Number: ……

Details of Images Required

Date: ……..

Time: ……

Camera Location: ……

Camera Number: ……..

Tick as Appropriate

I require viewing the images only ☐

I require a hard copy of the images ☐

Data Protection Declaration

I declare that the information given is correct to the best of my knowledge and that I am entitled to apply for access to surveillance camera images.

Records referred to above under the terms of the Data Protection Act 1998

Name: ……

Signature: ……

Date: ……

Annex C

Viewing of Surveillance Camera Images

Date & Time Viewed	Camera Number	Operator

Reason for Viewing:
Authorised By : Name: Signature:

Details of Person Viewing:

Name:

Appointment:

Signature:

Annex D

PROVISION OF IMAGES TO POLICE/ 3rd PARTY FOR INVESTIGATIO/ LEGAL PROCEEDINGS

Name of Applicant……

Company……

Telephone Number……..

Date of Incident……

Time of Incident……

Camera No……..

Location……

Crime/Incident Number……

Brief Description of Incident:
……
……
……
……
……
……

Signature……..

Date……..

Date of Destruction……

Method of Destruction……

Name of Person Carrying Out Destruction……..

Signature……

Annex E

Surveillance Camera Daily Check Sheet

Date	Time	Operator	Signature	Camera Date/Time Check	Picture Quality	Maintenance Contacted
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						