South East Coast Ambulance Service NHS
NHS Foundation Trust

CCTV (Buildings) Policy

Contents

1 Statement of aims and objectives

1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) is committed to ensuring, as far as is practicable and reasonable, the safety and security of Trust employees and those that come into contact with the Trust as the result of its activities. This is particularly emphasised in relation to the prevention and investigation of incidents of violence on members of staff. The Trust is committed to deterring those who may be minded assaulting members of staff wherever possible, and where this has occurred, to seeking and achieving the strongest forms of sanction and redress available.

1.2. The Trust is also committed to protecting its physical assets, such as its vehicles and the equipment stored on them, from theft and vandalism. Where practicable and where this does not compromise the Trusts' commitment to the safety and security of the staff and general public, it will strive to ensure that such acts against these assets are prevented, and in the case of occurrences, investigated as fully as possible.

1.3. With the use of CCTV on its sites and property, the Trust aims to provide a visible deterrent to all would-be offenders and provide re-assurance to staff, contractors and members of the public. The main content of this document stipulates how the Trust will manage, limit and control the deployment of Closed-Circuit Television (CCTV) throughout the headquarters and sites in use by the Trust. This policy aims to:

- Document and inform stakeholders, staff and the public about the deployment of CCTV at Trust sites.
- Detail the specifics regarding the extent and use of CCTV and the safeguards and limitations of its operation.
- Emphasise access controls to the resulting recorded video imagery in order to prevent inappropriate use.

1.4. It is noted that this policy is separate and distinct from the Trust's CCTV (Vehicles) policy and that the use and application of these separate CCTV systems differ.

1.5. This policy applies to all staff employed by the Trust, its' volunteers, stakeholders, contractors, members of the public and any other NHS Professional or Emergency Service Operatives, who may through the course of their duties or circumstance find themselves visiting Trust property.

2 Principles

2.1. The Trust will ensure that procedures and systems are in place to facilitate our legislative and regulatory obligations, which namely:

- Data Protection Act 1998
- General Data Protection Regulation 2018
- CCTV Code of Practice, as produced by the Information Commissioner and revised in 2008
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 1998
- Caldicott Report 1997

2.2. The Trust defines CCTV as 'the use of video cameras to record and store video imagery'. It is recognised that the term 'video imagery' can mean recordings of varying quality and can sometimes include recorded sound. For the purpose of this policy there will be no recorded sound data and that the quality is at least that of the lowest standard that is acceptable to be used as police evidence.

2.3. In line with the requirements of the Data Protection Act and General Data Protection Regulations, recording and storage of images / data is allowable on Trust sites and property on the understanding that information is processed only for the prevention or detection of crime; and the apprehension or prosecution of offenders.

2.4. All request types, as below, can only be authorised for retrieval and release by the Security Manager or nominated Deputy.

2.4.1. A member of public can see their data on receipt of a written request in line with subject access requests, to the Patient Experience Team.

2.4.2. A member of staff can request data if they believe a criminal offence has occurred. This request must be in writing to the Security Team, and accompany a completed CCTV access request form, who will only process the data if they are in agreement that a criminal offence may have occurred.

2.4.3. Security Management will process written requests from the police in line with their own investigations into a criminal offence provided accompanied by a countersigned S29 (3) Data Protection Act Form. Security Management will also liaise with the police and assist with any subsequent investigation arising.

2.5. **The Information Commissioner:** The Trust will notify the Information Commissioner of all personal data that is processed by the Trust for purposes not defined as exempt by the Information Commission. The Trust's use of CCTV is not exempt and as such, is routinely included in the Trust's annual renewal of its notification to the Information Commissioner. The notification includes:

2.5.1. The purposes for which personal data are being or are to be processed.

2.5.2. A description of the data subjects about whom data are or are to be held.

2.5.3. A description of the data classes e.g., personal details, financial details etc.

2.5.4. A list of the recipients of data.

2.5.5. Information about whether data are transferred outside the European Economic Area (EEA).

2.6. **Regulation of Investigatory Powers Act (RIPA) 1998:** The CCTV employed by the Trust will not be covert or directed in nature, and as such RIPA does not apply.

2.7. **Siting of Cameras**

2.7.1. When an offence is committed, the CCTV footage will be used as evidence to achieve successful prosecution and subsequent sanction and redress. It will aid investigations into thefts and violence, assisting the Trust in its commitment to protect staff, patients and the public as well as its own property and equipment.

2.7.2. The location of all CCTV cameras on Trust sites must be carefully considered. All areas covered must be that which is intended to be monitored in line with the Trusts' purpose on CCTV use.

2.7.3. Where it is not possible to restrict coverage to be limited only to property belonging to the Trust, the owner of the property or space must be consulted.

2.7.4. If the cameras are adjustable, they will be prevented from being manipulated to overlook areas not intended to be overlooked (i.e. property not belonging to the Trust).

2.7.5. All Operators of CCTV, where it is adjustable, must be aware of recognising privacy implications and the Trust policy for CCTV use.

2.7.6. In line with the overt nature of the CCTV, and to act as a deterrent in line with the Trust purpose for CCTV use (see 1) the cameras must, wherever possible, be sited in prominent positions in public and staff view.

2.8. **Signage**

2.8.1. Signs must be displayed to inform individuals that they are in an area where they are being recorded.

2.8.2. The signs will be clearly visible and readable and will:

2.8.2.1. Contain details of the organisation operating the system, and the purpose for using CCTV.

2.8.2.2. State who to contact about the scheme (where these things are not obvious to those being monitored).

2.8.2.3. Be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

2.8.3. An example of the wording as suggested by written guidance is “Images are being monitored and recorded for the purposes of crime prevention and public safety. This scheme is controlled by South East Coast Ambulance Service NHS Trust. For more information, call 01234 567890.”

2.8.4. Where visitors have difficulty seeing text they will be advised by the reception or Trust escorts of the presence of CCTV.

2.9. **Quality**

2.9.1. There will be no sound recording as this would make the CCTV and the information recorded intrusive in nature.

2.9.2. In order to be fit for purpose the images produced by the CCTV must be as clear as possible and at least the minimum specifications for what would be acceptable for use as evidence.

2.9.3. The equipment and recording media will be maintained on a regular basis to ensure the quality of the images is upheld.

2.10. **Storage and Retention of Data**

2.10.1. When images are retained, it is essential that their integrity be maintained to ensure their evidential value and to protect the rights of people whose images may have been recorded. Access to and security of the images will therefore be controlled in accordance with the requirements of the Data Protection Act 1998 and the Trust’s Record Management and Retention Policy.

2.10.2. When CCTV footage is not retained within a certain length of time (as outlined by the equipment type in the CCTV procedure), the CCTV recording equipment must automatically erase or record over this footage so as to prevent the storage and retention of inappropriate records.

2.11. **Access to and disclosure of images**

2.11.1. As in 2.4. all requests, can only be authorised for retrieval and release by the Security Manager or nominated Deputy.

2.11.2. Access requests within the Trust must be requested using a CCTV Access Form (Appendix A) and submitted to the Security Team for approval.

2.11.3. The Trust will only retain and use CCTV images in line with the purposes outlined in section 1 and where the conditions in 2.3 to 2.5 are met.

2.11.4. Where an individual requests to access records of their own personal data as captured by the CCTV footage, this must be done so in writing to the Patient Experience Team as the department handling patient

requests. These requests will be considered in line with other Third Party's rights and ongoing criminal investigation, where applicable. Where the release of footage may compromise such an investigation, disclosure may be delayed or refused, as appropriate.

2.12. **Subject Access Requests**

2.12.1. In the event of such a request the member of the public shall be provided with a standard subject access request letter.

2.12.2. A charge may be levied in respect of the request up to a maximum of £10 to cover the costs of dealing with the request.

2.12.3. The Corporate Information, Information Governance Manager will be responsible for considering any such requests in the light of the Data Protection Act 1998, guidance set out in the CCTV Code of Practice issued by the Information Commission and using the process laid out in this policy and accompanying procedure.

2.13. **Maintenance and Storage of CCTV equipment and data**

2.13.1. CCTV equipment / cameras will be maintained by the Estates Department to ensure they remain operational and are able to capture high quality footage to a sufficient level.

2.13.2. CCTV footage will be stored within a server room or on a password protected IT system (such as one requiring an 'admin' password), to ensure access to data is available in response to requests to the Security Team.

3 Definitions

3.1. It is recognised that any CCTV sited on Trust property will record personal information. The Trust defines personal information in accordance with section 2 of the Data Protection Act as "data which relates to a living individual" who can be identified:

3.1.1. From that data; or

3.1.2. From that data and other information, which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

3.2. It is also recognised that the data being processed may commonly contain specifically sensitive personal data, which is defined by the Trust in accordance with section 2 of the Data Protection Act as including:

- Gender
- Ethnic origin or race

- Political opinion
- Religious beliefs
- Trade union membership
- Health – mental or physical
- Sexual life
- Commission of any offence (or alleged)
- Any court proceedings or findings

3.3. The Trust states and defines that CCTV will be used "for the purposes of crime prevention and prosecution of offenders".

4 Responsibilities

4.1.1. The Executive **Director of Nursing & Quality** is the Director delegated with the responsibility for ensuring compliance with and monitoring of our CCTV policies within the Trust.

4.2. The **Security Manager** will oversee the implementation of this policy and will be responsible for the day-to-day implementation.

4.3. The **Security Coordinator** will administrate, record and coordinate CCTV buildings requests whether internal or external with the Police.

4.4. The **Head of Estates** is responsible for ensuring the CCTV cameras are maintained in accordance with Section 2.15.1.

4.5. The **Head of Information Technology (IT)** is responsible for ensuring CCTV footage is securely stored where it is housed in their department and accessible on request by the ASMSs in accordance with 2.15.2.

5 Competence

5.1. The Trust have a Security Team to advise on all matters relating to the security of staff. All operators of CCTV, where it is adjustable, must be aware of the importance of privacy under the Data Protection Act and the use of CCTV only for its sole purpose as defined by Trust in this policy.

6 Monitoring

6.1. All CCTV surveillance will be automatically recorded and any breach of the Data Protection Act or the codes of practice or this policy will be detected via the controlled access to the system and auditing. The access will be controlled and documented by Security Team.

6.2. A copy of all requests for CCTV access will be stored by the Security Team and will be available in the event for any need to audit or review.

6.3. In addition the Security Team will formally inspect the CCTV systems for any breaches of access where a risk or issue has been identified and submit that report to the Health & Safety Committee.

7 Audit and Review

7.1. The policy will be reviewed every three years by the Security Manager, or earlier in the light of changing circumstances or legal requirements, any changes will be made following the requirements set out in the Trust's Policy for the Development and Management of Trust Policies and Procedures.

7.2. The internal auditors on request and aided as necessary by relevant technical specialists, will carry out periodic audits on individual sections/departments of the Trust responsible for the operation of the CCTV units and the implementation of this policy. This is to provide assurance to the trust via the Health & Safety Committee that a suitable standard is in place and is functioning correctly. Technical equipment, as well as methods of working, are also to be covered in by the audit.

8 References

- Data Protection Act 1998
- General Data Protection Regulation
- CCTV Code of Practice, as produced by the Information Commissioner and revised in 2008
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 1998
- Caldicott Report 1997

Appendix A: CCTV Access Request Form

CCTV Access Request Form

Form for requesting CCTV records

This form MUST be submitted in ALL cases where CCTV footage is requested and provided to the Security Team for Approval. For further details, please see SECAmb the CCTV Policy.

Requesting Officer Details

Title:

First Name: **Surname:**

Job Description: **Station/Locality/HQ:**

Specific information required e.g. What information is sought, which vehicle/building etc. please also include any individuals (where known) that will be either intentionally or unintentionally included. Also, explain briefly what is on the tape that requires viewing. Please note that sound is not recorded. Please see CCTV (vehicles) or CCTV (buildings) policy for guidance (as appropriate)

(continue overleaf if necessary)

Date:

Start time: **End Time:**

CCTV can only be viewed or downloaded in the instances where the law has been broken, or there is reason to believe so. Please state briefly how this incident fulfils this criteria:

Date Required:

/ / 20__

Note: ASAP is not appropriate please provide a realistic date and the Risk Department will make best efforts to complete within timescale.

Requesting Officer:

Signed …… Date: / / 20__

Authorisation

Security Team Authorisation:

Access request: **Accepted** **Rejected** **(ring as appropriate)**

Print Name…… Signed ……

Date received : / / 20__ Date completed : / / 20__

Date viewed: / / 20__

Comments:

Viewer Audit – to be used to record ALL people who view footage - not including external parties, such as the Police, Coroner or Data Subjects (where the formal requesting process has been followed)

Print Name…… Signed ……

Date viewed: / / 20__

Print Name…… Signed ……

Date viewed: / / 20__

Print Name…… Signed ……

Date viewed: / / 20__

Print Name…… Signed ……

Date viewed: / / 20__

(continue overleaf if necessary)