South East Coast Ambulance Service NHS
NHS Foundation Trust

CCTV (Vehicle) Policy

Contents

1	**Introduction**	2
2	**Aims and Objectives**	2
3	**Definitions**	2
4	**Policy Statement**	3
5	**Competence**	3
6	**Arrangements**	4
7	**Responsibilities**	10
8	**Competence**	12
9	**Monitoring**	13
10	**Audit and Review**	13
11	**Equality Analysis**	13
12	**References**	14
13	**Appendix A: CCTV Access Request Form**	15
14	**Appendix B: CCTV retrieval and software authorisation form**	16

1 Introduction

1.1. This policy applies to all staff employed by South East Coast Ambulance Service NHS Foundation Trust (the Trust), as well as 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 in Trust ambulance vehicles.

1.2. CCTV will not be used to performance manage staff, but will be used in relation to the prevention and detection of crime to protect staff and patients against violence and aggression, for the security of Trust assets, vehicles and equipment and to support Road Traffic Collission (RTC) investigations and allegations of poor driving standards.

2 Aims and Objectives

2.1. This policy aims to:

- Ensure the Trust's use of vehicle CCTV is in line with all statutory requirements.
- Detail the conditions and operation for the appropriate authority, use, retrieval, storage and management of footage.

3 Definitions

3.1. The Trust defines CCTV as 'the use of recording video cameras to store time and date stamped data as video imagery'.

3.2. Security authorisation is defined as the Lead for Security or suitable qualified deputy providing authorisation for requests, for others to approve requests or retrieve CCTV for any incident. Fleet authorisation is defined as the Head of Fleet and Logistics or suitable qualified deputy in their absence providing authorisation for requests, or to retireve CCTV in relation to RTCs and allegations of poor driving standards.

3.3. The Trust uses a variety of systems and software on its vehicles as supplied by systems operator and supplier. This software is under the control of IT but may only be supplied to an approved user, on the authority of the Lead on Security or their nominated deputy.

3.4. An approved user will be part of a named group of individuals authorised by the Lead on Security and only where there role involves handling matters of security (i.e. the Lead on Security or a qualified deputy) or RTCs/drving standards (i.e. Fleet On-Call Management and associated IT Communications support).

4 Policy Statement

4.1. South East Coast Ambulance Service NHS Foundation Trust is committed to ensuring, as far as is practicable and reasonable, the health, safety and welfare of Trust employees and those that come into contact with the Trust as the result of its activities.

4.2. This is particularly emphasised in relation to the prevention and investigation of incidents of violence against members of staff. The Trust is committed to deterring those who may be minded to assault members of staff wherever possible, and where this has occurred, to seeking and achieving the strongest forms of sanction and redress available. Therefore the Trust has adopted CCTV to support the criminal justice system and to bring perpetrators to justice.

4.3. The Trust is also committed to protecting its physical assets, such as

4.4. Vehicles and the equipment stored on them including medicines and medical gases, from theft and vandalism or damage as a result of a collision or incident.

4.5. Where an RTC or allegation of driving standards occurs, there is also a responsibility of the Trust to utilise footage to support investigations, internally, with the Police or the Trust's insurers.

4.6. It is recognised that the presence of CCTV, and signs detailing its use, may also act as a deterrent to those who might engage in criminal acts through the possibility that images captured will be used in their prosecution and conviction.

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

4.8. It will also be used to support investigations following an RTC or allegations of poor driving standards and will be used as a learning tool to prevent further collisions and improve driving standards.

5 Competence

5.1. The Trust will ensure at the relevant levels that a request process is in place and that only upon appropriate authorisation is footage retrieved, whilst ensuring any Trust management are aware of their information governance responsibilities whilst in possession and operatives

completing maintenance on systems does not infringe on data subjects rights.

6 Arrangements

6.1. This policy complies with both Trust and statutory requirements of the documents referenced in the associated documents and reference sections of this document respectively. Explicit areas of legal requirement and relevant responses are stated below with regard to:

6.2. ***The Data Protection Act 1998*** Due to the potentially contentious, graphic and sensitive nature of the video imagery recorded by any CCTV recording device and the laws of data protection for sensitive personal information, recording and storage of such information is allowable on Trust vehicles on the understanding that information is processed only for the following purposes:

- The prevention or detection of crime including:
    - To support the prosecution of offenders for assaults to staff
    - To detect and support the prosecution of offenders for criminal damage to Trust assets such as equipment or vehicles.
    - Support the security and prevention of theft of medicines and medical gases.
    - The apprehension or prosecution of offenders relating to security incidents such as violence and aggression, criminal damage.
    - To support investigations following an RTC, vehicle related incidents or allegations of poor driving standards.
- Recorded information will only be used following formal written request to theTrust Lead on Security or nominated deputy who can authorise any request or, one of the On-call Fleet Managers who can authorise only RTC and/or Driving Standards requests; and in one or more of the following circumstances:
    - A specific criminal offence has occurred.
    - The Lead on Security has reasonable grounds to believe a specific criminal offence has occurred.
    - An allegation of inappropriateness has been made where viewing the footage can confirm or refute the allegation.
    - Following a request from the Police or other legal authority in line with their own investigations into a criminal offence.

- Where a data subject has made a written request to view their own personal information within the CCTV records.

- Out of hours and in exceptional circumstances and only where it is **essential** that the CCTV records are examined before the Lead on Security or an On-call Fleet Manager is available and in accordance with the associated crime prevention/detection principles and required forms covered in this policythen the Tactical On-Call Manager can authorise viewing and downloading of the footage with support from the On-Call IT Communications Management where required. In these cases a written record describing the reason and circumstances must be submitted to the Lead on Security as soon as reasonably practicable This process will ensure that an effective audit trail is maintained which will withstand scrutiny and complies with the *Data Protection Act.*

- The Trust will be prepared to deny requests where the legal authority to request footage is not sufficient and/or in line with the principles of crime prevention/detection as covered earlier in this Policy.

6.3. **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, must be informed to the Information Commissioner on inception and if any significant changes occur. An increase of cameras or the number of vehicles will not constitute a significant change however the following but not limited to would, including increased range of the lens, type of lens e.g. infra red, length of retention before overwriting etc. or any significant change to the governance or policy.

6.4. **The Road Vehicles (Construction and Use) Regulations 2003** The use of CCTV in Trust vehicles must not cause or permit any other person to drive a motor vehicle on a road while that other person is using a device, other than a two-way radio, which performs an interactive communication function by transmitting and/or receiving data. This includes sending or receiving still or moving images.

6.5. ***Regulation of Investigatory Powers Act 2000*** *The Regulation of Investigatory Powers Act 2000 ("RIPA")* regulates the manner in which certain public bodies may access a person's electronic communications and conduct surveillance (such as CCTV recording).

In the extreme circumstance the Trust considers such a measure all requirements of this Act must be adhered to.

Whilst the overriding principle concerning provision of CCTV in vehicles for detection of crime is consistent in both this Policy and the RIPA act, the CCTV employed by the Trust will not be covert and as such is not intrusive nor directed in nature as defined by the act. As such RIPA does

not apply for the Trust provision and use of Vehicle CCTV as outlined in this document.

6.6. **Signage and notification of activation** Signs must be displayed to inform individuals that they are in an area where they are being recorded.

The signs will be clearly visible and readable and will contain details of the organisation operating the system and the purpose for using CCTV detailing that CCTV may recording or similar inference and who to contact about the scheme.

CCTV will beging recording when the ignition is turned on and may remain recording for a period of up to 60 minutes after the ignition is turned off depending on power/warm down times of the system.

6.7. **Recordings** 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.

The equipment and recording media will be tested/maintained on a regular basis by either authorised Fleet Operatives or specialist contratractors to ensure the quality of the images is upheld, whilst at the same time not accessing footage stored on the system. As such any viewing of CCTV will be restricted to five minutes before the time of access to ensure only the vehicle in the garage is witnessed.

The recorded footage must be date and time stamped accurately on the footage itself; so as to give a basis of the time and date each recording was made.

Recording of CCTV footage must continue uninterrupted filling up to its storage capacity and automatically recording over itself in a continuous function.

Where a recording is accessed and has footage concerning an alleged offence that would be used as evidence, the recording must be stored and handled securely as is required for continuity of evidence for prosecution in a locked filing cabinet, with its movements recorded prior to handover to the police as evidence.

6.8. **Storage and Retention of Footage** When footage is 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 1998 Data Protection Act and the Trust's Data Protection Policy.

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.

After footage is accessed and stored the data must either be:

- Retained by the police or Trust as evidence under the Police and Criminal Evidence Act.
- Deleted/Destroyed at the end of the investigation for which it was first retained.

CCTV footage, in all forms both on the vehicle and stored off it, is subject to the Trust's Removable Media: Information Security Policy

6.9. **Access, retrieval and disclosure of footage** Overarching authority for the access, viewing, retrieval of footage and associated software sits with the Trust Lead on Security. All security related requests and those outside RTCs/Driving standards must be authorised by the Trust Lead on Security or a suitably qualified deputy in Security Management in their absence.

The Head of Fleet and Logistics has autonomy in relation to the access, viewing, retrieval of footage and may authorise such requests, but only in relation to RTCs/driving standards. The Head of Fleet and Logistics may also delegate responsibility for retrieval to any of the named On-Call Fleet Managers.

It is recognised that to support a timely and efficient progress of requests and/or investigations requiring CCTV, those authorised by the Trust Lead on Security to retrieve footage may support each department. As such any individual authorised to retrieve footage will ensure an enhanced DBS check is completed.

There will be scope for other specialist non-operational employees who are both enhanced DBS checked, have received authorisation by the Trust Lead on Security and had training to support security and fleet where an urgent matter requires resolution with footage retrieved to ensure statutory requirements are met.

Access requests within the Trust must be requested using a CCTV Access Form (see Appendix A) and submitted to the Lead on Security, their nominated deputyor Head of Fleet and Logistics for approval, out of hours and in exceptional circumstances this can be approved by the Tactical / Regional Operations Manager who must then submit the request form to the Lead on Security.

The CCTV Access Form must be stored alongside the footage and updated as the footage is used. Once the footage has been destroyed the form must continue to be retained by the requestor and a copy sent to and stored by the Lead on Security or their nominated deputy.

Disclosure of CCTV relating to matters of crime prevention / detection may only be disclosed outside the Trust by a member of Trust Security Management and only to a law enforcement agency.

Disclosure of RTC footage may be disclosed outside the Trust by either a member of the Fleet Insurance Department or one of the On-Call Fleet Managers and only to the Trusts insurers, or again to a law enforcement agency.

Disclosure of CCTV as part of a named subject access request may be completed by a member of the Patient Experience Department but only to the data subject or authorised representative.

Only those authorised by the Lead on Security (and including the Lead themselves) may remove footage from vehicle CCTV units, must be used as described in this document and may not be used for learning and development purposes.

6.10. **Informing recorded parties of viewings** Where necessary, employees of the Trust and patients/members of the public who are subject to visual presence on any footage will be informed that CCTV has been accessed to be viewed.

The following mitigating circumstances however may prevent or prompt the Lead on Security to decide not to inform employees or members of the public concerning the use of CCTV with their images. This includes but is not limited to:

- The individual is suspected of involvement in any criminal matter being investigated.
- The individual is not identifiable, details of them are not known or they cannot be contacted.
- Where doing so might exacerbate or prompt extreme or unacceptable behaviour (e.g. where an individual is known to have already been violent, and informing him of the CCTV viewing may possibly prompt this behaviour).
- Where a lawful authority requests parties are not informed and, as an appropriate lawful authority, invokes the RIPA Act to perform surveillance that is covert, intrusive or directed through SECAmb vehicles or recording devices.
- Where doing so might induce a conflict of interest or impede the legal process.

The decision not to inform parties of CCTV footage being viewed does not make the surveillance covert due to the provision of adequate signage within the vehicle highlighting its use.

The above conditions relates to accessing and viewing CCTV by the Trust “for the purposes of crime prevention and prosecution of offenders” and does not apply or conflict with subject access requests for footage and the conditions pertaining to them.

6.11. **External Requests for footage** The Trust also recognises that there will be other circumstances where, to comply with lawful authority, the Trust will be made to comply with requests from external parties – this might include (but is not limited to) circumstances where:

- The Police, Coroner, HM Customs or other law enforcement bodies. make a request for footage based on investigations which the Trust and its employees/patients may or may not be directly linked. In such cases the appropriate authority would be required, such as a countersigned section 29(3) Data Protection Act form in the case of the the Police, even where Trust employees are the victims.

- Where footage is required by Security Services in the interests of national security. In such cases the overarching public interest tests and duties to the state may supersede other legislation.

- Where other lawfully authorised parties such as the Trust's insurers require footage to support, defend, exonerate staff etc in relation to RTCs.

6.12. **Subject Access Requests** Members of the public are entitled to make requests under the Data Protection Act for copies of footage of themselves held as a result of CCTV recordings.

In the event of such a request the member of the public shall be provided with a standard subject access request letter and will be expected to provide confirmation of identity.

For any access request to be considered, the Trust will require the following details:

- The date and time of the event. (The requestor may only receive CCTV for footage they are contained in and relating to their treatment or care).

- Information regarding the vehicle (call sign, registration, fleet number or the crew on this particular day).

Access requests for CCTV made more than a three weeks after the event shall be automatically responded to stating that the footage will have been recorded over, as is what current system capacity allows.A charge may be levied in respect of the request in line with Data Protection Act to cover the costs of dealing with the request.

Where a Subject Access Request takes place, the Trust is obliged to ensure no one except the individual making the request appears in the image(s) and Recordings(s) shared, and that no other data which does not relate to the subject is shown (for example – other parties or employees, patients, details of any treatment or any views out of the rear of the ambulance if the doors are open etc.)

6.13. **Reporting** All incidents where the CCTV recording has been requested must follow from the submission of a Datix form. This may be included within the same Datix form that highlights the incident that resulted in the request for CCTV footage download.

7 Responsibilities

7.1. The **Chief Executive Officer** is accountable for:

- Promoting and supporting the aims and objectives of this policy.
- Ensuring that there are arrangements for identifying, evaluating and managing risk associated with CCTV usage within the Trust.
- Providing resources for putting the policy into practice.
- Ensuring that there are arrangements for monitoring incidents linked to CCTV usage in the Trust and that the Board reviews the effectiveness of the policy.

7.2. The **Director of Nursing and Quality** is responsible for:

- Promoting and reporting security management issues to the Trust Board, including those where CCTV has been used.
- Ensuring that full cooperation is given to the police (or any other lawfully authorised body) in any investigation requiring use of CCTV footage.
- Ensuring that in the event of any adverse incident involving CCTV systems are in place to ensure an investigation can be completed and that any statutory authority is advised where appropriate, e.g. the Information Commissioner.

7.3. The Security Department is responsible for:

- Liaising with the Police or any other lawful authority with regard to supplying or responding to requests for CCTV footage in relation to security incidents of violence, aggression or criminal damage etc.
- Assisting with any subsequent investigation.
- Undertaking an investigation where the Police are unwilling to do so and where the Trust's Security Management Director requests intervention by the Lead on Security and using CCTV footage appropriately to do so.
- Providing security advice on an ad-hoc basis to the Trust with regard to use of CCTV and its implementation.

- Retrieval and secure storage of CCTV data that has been subject to retention for scrutiny and a record relating to the footage.

- Approving any requests for access to CCTV footage within the timeframe outlined by the CCTV Procedure

- Maintaining the security of the software for viewing once the footage is retained, through use of encryption and password protection wherever possible.

- Ensuring that footage they have retained is deleted/destroyed at the end of the investigation for which it was first retained.

- Ensuring that all records recording CCTV Access requests and subsequent use are up to date and securely stored.

7.4. The **Head of Fleet and Logistics is** responsible for, in relation to road traffic incidents:

- Liaising with the Police or any other lawful authority with regard to supplying or responding to requests for CCTV footage for RTCs or matters of driving standards.

- Assisting with any subsequent investigation.

- Approving requests for access to CCTV footage only for RTCs or matters of driving standards within the timeframe outlined by the CCTV Procedure

- Ensuring a Local Operating Procedure (LOP) exists for maintenance of the physical system onboard ambulances.

7.5. The **On-Call Fleet Managers** are responsible for, in relation to road traffic incidents:

- Liaising with the Police or any other lawful authority with regard to supplying or responding to requests for CCTV footage in relation to RTCs or driving standards.

- Assisting with any subsequent investigation.

- Retrieval and secure storage of CCTV data that has been subject to retention for RTCs or driving standards.

- Maintaining the security of the software authorised by the Trust lead on Security for viewing once the footage is retained, through use of encryption and password protection wherever possible.

- Ensuring that footage they have retained is deleted/destroyed at the end of the investigation for which it was first retained.

- Ensuring that all records recording CCTV Access requests and subsequent use are up to date and securely stored.

7.6. The **Patient Experience Team** is responsible for:

- Dealing with Subject access requests.
- Providing advice, where required, to the Lead on Security on the legitimacy of requests and lawful authority to make them.
- Liaison with the information Commission, (as described in section 5.3) concerning data processing within the Trust

7.7. The **Fleet Department** is responsible for:

- Fitting and retrofitting all appropriate vehicles for CCTV with the means to do so.
- Upkeep and maintenance on CCTV cameras and related equipment for their use to ensure they remain operational and are able to capture high quality data to a sufficient level.
- Responsible for removal of vehicle hard drives and their secure transport to the appropriate site for security review and download.

7.8. The **IT Department** is responsible for:

- Installing and updating approved secure software for Secuirty Management, the Fleet On-Call Managers and any other Managers approved by the Trust Lead on Security to view retained CCTV data.
- All staff are responsible for adhering to the policy and processes.

8 Competence

8.1. The Trust have employed Security Management to advise on all matters relating to the security of staff.

8.2. The Trust Lead on Security (or other senior member of the Compliance Department in their absence as defined in 6.9.1) must be aware of the importance of privacy under the Data Protection Act and the use of CCTV and any footage only for its sole purpose as defined by Trust in this policy.

9 Monitoring

9.1. All CCTV footage 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 Lead for Security for controlled access to the system and auditing.

9.2. Where required a report of specific instances of retention of vehicle CCTV footage will be submitted by the Lead on Security or Head of Fleet and Logistics to the Central Health and Safety Working Group, and justification provided for its use. Records of this will be included in the minutes.

9.3. All CCTV access request forms, whether approved or rejected, and alongside the accompanying corresponding viewer audit, will be stored securely by the Lead for Security or Head of Fleet and Logistics for a period of six years after the application, to demonstrate compliance with the principles of this policy.

10 Audit and Review

10.1. The policy will be reviewed at least every three years by the Trust Lead on Security, or earlier in the light of changing circumstances or legal requirements. Any changes will be made following the process set out in the Policy and Procedure for the Development and Management of Trust Policies and Prcoedures.

10.2. 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 to provide assurance to the trust via the Quality and Patient 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.

11 Equality Analysis

11.1. The Trust has undertaken an Equality Analysis (EA) and those consulted were assured that appropriate governance would be in place to ensure no protected characteristics would be infringed by this policy.

11.2. Due regard is given to the link between this policy and the need for protocols to capture the incidence of hate crime, linked to protected characteristics, directed at Trust staff e.g. Racial abuse. The EA also identified positive impacts on those with the protected characteristics of Age, Disability, Gender reassignment and Pregnancy and maternity.

11.3. The possible negative impact of the system is that one of the cameras covers the clinical treatment area of the vehicle. It is considered that the policy seeks to balance risk and proportionality – risk to patient care against our statutory duty to provide a safe working environment for our

staff. However controls are in place to mitigate impact with this policy ensuring;

11.4. The internal camera is only viewed/retrieved where there are issues of crime prevention detection

11.5. The internal camera may not be routinely reviewed or footage retrieved for RTCs or matters of driving standards, unless authorised by the Trust Lead on Security (or forms part of a data subjects request)

11.6. Trust representatives authorised to view/retrieve footage will also be required to have an enhanced DBS check.

12 References

12.1. Data Protection Act 1998

12.2. CCTV Code of Practice, as produced by the Information Commissioner and revised in 2008

12.3. Home Office Surveillance Camera Code of Practice June 2013

12.4. Protection of Freedoms Act 2012

12.5. Regulation of Investigatory Powers Act 1998

12.6. The Road Vehicles (Construction and Use) Regulations 2003 (Amended)

12.7. Caldicott Report 1997

Appendix A: CCTV Access Request Form

This form must be completed for any CCTV footage requested internally and provided to the Security Team for security/internal investigation related request or the Fleet Team where the matter relates to an RTC or driving standards matter. Criteria for requests can be found within the CCTV (Vehicles) and CCTV (Buildings) Policies.
Requesting Staff member details
First Name: Surname: Job Title: Location: Details of incident: Date: / / 20__ Start time: End Time: Vehicle fleet number/Callsign: IWR1 Ref:
Reason for request:
Date Required: / / 20__ Note: ASAP is not appropriate please provide a realistic date and the Security/Fleet Team will make best efforts to complete within the timescale provided.
Requesting Staff member: Signed ……. Date: / / 20__
Security / Fleet Team Authorisation: Access request: Accepted Rejected (ring as appropriate) Print Name…… Signed ……

A copy of this form must be printed and stored securely with the record of request.

14 Appendix B: CCTV retrieval and software authorisation form

Authorisation for retrieval of Trust Vehicle CCTV footage

Due to the nature of the work undertaken by the Trust there are occasions where evidence is required to satisfy statutory requirements in support of the State, Trust and / or its staff. For this reason, there is a requirement to identify individuals to be authorised to retrieve footage where crime prevention, detection or a road traffic collision has occurred.

This form, authorised by the Trust's lead on security, enables the user to operate and retrieve footage under the following conditions;

- The reason for viewing footage or retrieval of footage must be for only crime prevention, detection or a road traffic collision.
- The user is authorised to handle CCTV on Double Crewed Ambulances, Paramedic Practitioner vans and Single Response Vehicles.
- The user either has or will have prior to unsupervised viewing / retrieval ensured a sufficient enhanced DBS check has been completed.
- The user will limit the timeframe viewed and the rear cab camera viewed to a minimum but is recognised where justified to retrieve a sufficient level of footage.
- The user will not allow any other internal person, not involved in the event to view the footage without consulting with the Trust's Lead on Security and the CCTV form having been completed (See Vehicle CCTV Policy).
- Unneeded camera downloads (inc. email attachments) should be deleted as should all footage that is no longer required to be held. For cases going to Court it is accepted footage may need to be retained for an extended period.
- The viewing software (VUE, ATSR, Smart Witness) is authorised to the below named user only and must be kept secure.
- The user will adhere to all laws, policies and procedures relating to security of information and information governance.

Footage may only be disclosed to the Trusts Insurers without requiring prior consent. For all other disclosures, a CCTV form (internally) or Data Protection Act form (externally) may be required and so guidance and/or authorisation will be required from the Trust Lead on Security. All retrievals / disclosures other than to the Insurers must demonstrate crime prevention, detection or apprehension or prosecution of a suspect.

I accept the terms of this agreement and confirm I have the necessary requirements to be suitable as a user.

Print Name……..
Signature……
Job title……....

Authorised By Trust Lead on Security;
Print Name……...
Signature……