South Central Ambulance Service
NHS Foundation Trust

CLOSED CIRCUIT TELEVISION (CCTV) POLICY

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

DOCUMENT INFORMATION

Author:	John Dunn, Head of Risk and Security
Ratifying committee/group:	Health, Safety and Risk Group
Date of ratification:	24th March 2021
Date of Issue:	24th March 2021
Review due by:	March 2024
Version:	**V8**

Contents

1. Introduction

1.1 The Trust recognises its responsibilities under the Data Protection Act (DPA) 2018, the General Data Protection Regulation and associated data protection principles with regard to the use and operation of close circuit television (CCTV) recording systems within the Trust.

1.2 This policy sets out the Trust's arrangements with regard to the use, operation and management of the close circuit television (CCTV) recording systems within the Trust.

2. Scope

2.1 This policy applies to all staff within the Trust involved in the activation, viewing, use, operation, storage and management of CCTV located in either Trust buildings or vehicles; and/or whose images may be captured on the Trust's CCTV systems. It also applies to visitors, volunteers and members of the public who could be affected by the CCTV and/or whose images may be captured on the Trust's CCTV systems.

2.2 Patient Transport Service vehicles are currently not fitted with CCTV so this policy does not apply to those vehicles. However, it could apply to Patient Transport Service staff if, for whatever reasons, they were involved in the activation, viewing, use of CCTV whilst they were at work for the Trust; and if their images were captured by the CCTV systems in use within the Trust.

3. Equality Statement

3.1 The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marriage and civil partnership, disability, race, gender, religion/belief, sexual orientation, gender reassignment and pregnancy/maternity or any other basis not justified by law or relevant to the requirements of the post. The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of the afore mentioned protected characteristics, whether full or part time or employed under a permanent or a fixed term contract or any other irrelevant factor.

3.2 By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

3.3 Where there are barriers to understanding; for example, an employee has difficulty in reading or writing, or where English is not their first language, additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the Human Resources Department.

4. Aim

4.1 The aim of this policy is to set out the arrangements the Trust has in place with regards the use, operation and management of the CCTV systems in its premises and vehicles. It is also to ensure that the use, operation and management of the CCTV systems in Trust premises and vehicles and any images captured and recorded by these systems complies with the Data Protection Act 2018, the General Data Protection Regulation and all other relevant legislation concerning CCTV.

4.2 The policy also aims to ensure that:

- the use and operation of the CCTV within the Trust is for assisting with the maintaining of the security of Trust premises and vehicles; for preventing and investigating crime; assisting with the protection of staff; patients/service users or others whose image(s) may be captured; and assisting with the investigation of incidents involving:
    - staff being subject to abuse, or threatened or assaulted in the saloon of the vehicle;
    - and/or road traffic collisions involving Trust vehicles
    - and/or complaints
    - and/or concerns about patient safety
- all access, retrieval, viewing and use of the CCTV and any images captured is done in accordance with the Data Protection Act 2018, the General Data Protection Regulation and their respective principles and any other relevant legislation
- the sharing of any information captured by the CCTV is done in accordance with the Data Protection Act 2018 and the General Data Protection Regulation
- any images recorded are not to be used as part of any disciplinary procedure and/or capability procedure and/or in connection with any alleged clinical negligence and/or patient safety concerns against a member of staff unless they are in breach of section 7 of this policy. (Where an investigation take place, the member of staff involved has the right to request and review the images captured by the Trust's CCTV recording systems)
- all of the images recorded and information captured by CCTV is held, secured and disposed of in accordance with the Data Protection Act 2018 and the General Data Protection Regulation.

5. Roles and Responsibilities

5.1 Trust Board

5.1.1 The Trust Board will ensure that there are suitable and sufficient arrangements and adequate resources for the effective implementation of this and other associated policies.

5.1.2 It will also ensure that there are suitable and sufficient arrangements for the management of health and safety and the identification, assessment and management and control of risks to patients, staff, the general public (anyone affected by the activities of the Trust), Community First Responders, Contractors, Agency Staff and Bank Staff.

5.2 Chief Executive

5.2.1 The Chief Executive has overall accountability for ensuring that the Trust fulfils its legal responsibilities, and that the policy objectives are achieved and that effective machinery is in place for the achievement of the policies concerned with health, safety, welfare and security of staff and for the security of Trust premises.

5.2.2 He is also responsible for ensuring that:

- Trust policies are reviewed as appropriate in order to secure continuing compliance with existing policies, current legislation and any changes in the law
- the allocation of the resources necessary to maintain sound and efficient health and safety and security arrangements
- the effective implementation of this policy within the Trust and for ensuring that there are suitable and sufficient arrangements for the identification, assessment and management and control of the risks.

5.3 Executive Director

5.3.1 Executive Directors are responsible for the effective implementation of this policy within their directorates and for ensuring that there are adequate resources available to fulfil the requirements of this policy.

5.3.2 They are also responsible for the provision, application and monitoring of health and safety policies and procedures within their Directorate. They will ensure that all arrangements for the health, safety and security of staff, employed within their Directorate, are made known, maintained and reviewed whenever there is a change of operation, equipment or process.

5.4 Director of Patient Care and Service Transformation

5.4.1 The Director of Patient Care and Service Transformation is directly accountable to the Chief Executive and will advise and assist the Trust Board in fulfilling its duties under the relevant statutory legislation. In particular, the Director of Patient Care and Service Transformation, as the nominated Security Management Director (SMD) is responsible for:

- ensuring that workplace health, safety and welfare procedures are constantly reviewed
- ensuring that there are arrangements for liaising with the Health and Safety Executive (HSE)
- ensuring that the Trust Board are kept abreast of relevant new legislation, European Union Directives, Regulations, Approved Code of Practices (ACOPs) and British Standards, in order to ensure on-going compliance with the law
- keeping and maintaining a Corporate Risk Register
- the overall legal responsibility for the Trust's CCTV systems.

5.5 Managers and Supervisors

5.5. All Managers and Supervisors are responsible for:

- following any relevant guidance issued on the CCTV within the Trust and the Data Protection Act 2018 and the General Data Protection Regulation
- attending any training to enable them to fulfil their responsibilities outlined in this policy
- bring this policy to the attention of staff within their areas of responsibility
- ensuring that all staff within their area of responsibility comply with this policy and any associated protocols and procedures
- ensuring that all incidents involving a breach of security on Trust premises are reported on the Trust's Incident reporting systems, Datix.
- encouraging staff to report all incidents involving an activation of the CCTV systems within the Trust using the Trust's Incident reporting system, Datix
- ensuring that members of staff are given support following an activation of the CCTV as a result of a violence and aggression incident and/or a road traffic collision
- investigating, and/or arranging for the investigation of incidents following the activation of the CCTV and which involve their staff
- informing the Risk Team of any activation of the CCTV which involves their staff being assaulted and going off work (or incapacitated from doing their normal job of work) for over seven days
- notifying the Risk Team of any breaches of this policy and the Data Protection Act 2018 and the General Data Protection Regulation
- where necessary, seeking advice on the use and operation of CCTV within the Trust
- where necessary, referring any staff who have activated CCTV as a result of being subject to violence and aggression and/or a road traffic collision
- assisting with the development of a pro-security culture within the Trust.
- report any defects about the in-vehicle CCTV systems to the Operational Support Desk (OSD)

5.6 All Staff

5.6.1 All staff have the following responsibilities:

- to make themselves fully aware of this policy and abide by it
- to take reasonable care for their health and safety and that of others who may be affected by their acts or omissions
- to abide by any information, instruction and guidance provided to them in the use and safe operation of the Trust's CCTV system
- to, as part of their daily inspection of the vehicle, check that the in-vehicle CCTV systems, where fitted, is working
- to adhere to any safety measures put in place to ensure their safety, including any safe systems of work or safe operating procedures in relation to the Trust's CCTV system
- to activate the internal CCTV in Trust vehicles whenever it is necessary
- to report any activation of the CCTV system in/on Trust vehicles using the Trust's Incident reporting system, Datix

- to report any breaches of the use of the CCTV system and the Data Protection Act 2018 and the General Data Protection Regulation using the Trust's Incident reporting system, Datix
- to report all incidents involving a breach of security on Trust premises and vehicles
- to report any incidents involving being filmed by members of the public using the Trust's incident reporting system, Datix
- to comply with the Data Protection Act 2018, the General Data Protection Regulation and CCTV Code of Practice
- where necessary, provide the Police with statements
- to assist with the development of a pro-security culture within the Trust
- To report any defects about the in-vehicle CCTV systems to the Operational Support Desk (OSD).

5.6.2 Staff involved in the operation and access of the CCTV equipment will be made aware they are only able to use the equipment for the purpose stated in this policy.

5.7 Local Security Management Specialists/Risk Team

5.7.1 The Trust has one trained and accredited Local Security Management Specialist (LSMSs), namely the Head of Risk and Security.

- The Local Security Management Specialist (LSMS) are responsible for:
- maintaining an oversight of the Trust's CCTV systems
- advising, in consultation with Estates and SCFS Ltd, on the specification of the CCTV systems in use within the Trust
- advising on the use and operation of the CCTV systems within the Trust which should only be used in accordance with this policy
- advising on the procedures supporting their operational use to ensure compliance with NHS England and NHS Improvement guidance
- providing assurance to the SMD that the requirements set out in that guidance are met.
- for maintaining secure access to all recordings which may be captured by the vehicle saloon CCTV recording system
- for maintaining secure access to any external recording which may be captured as a result of non-driving incidents such as violence and aggression incidents.

5.7.3 The Local Security Management Specialist, together with other members of the Risk Team, are responsible for:

- the removal and secure storage of any hard disk/flash card following any incident in the saloon and for the installation of a replacement
- the retrieval, downloading and secure storage of any SCAS CCTV images recorded and stored on the remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd in relation to any violence, aggression, security incidents or patient safety incidents.

5.8 Head of Estates

5.8.1 The Head of Estates is responsible for:

- the installation and maintenance of CCTV recording systems within Trust premises in consultation with the Trust's LSMS
- keeping and maintaining an asset register of each of the CCTV recording systems installed in Trust premises
- ensuring that Operator's manuals are located and available in every Trust premises that has CCTV recording systems installed
- ensuring that the images captured and recorded by the CCTV recording system installed in Trust premises are of an appropriate quality
- ensuring that a record of inspection, maintenance and repair work in respect of the CCTV recording system in Trust premises is held and maintained; and is available for inspection and audit purposes; these records should be held for the lifetime of the CCTV recording system
- ensuring that a record of the viewing of the CCTV recording systems installed in Trust premises is held and maintained; and is available for inspection and audit purposes
- informing and discussing any intended changes to the CCTV recording systems installed within Trust premises with the Trust's LSMS and the Information Governance Manager; for instance, the installation of new CCTV recording systems within Trust premises or the removal of CCTV recording systems from Trust premises.

5.8.2 The Head of Estates is also responsible for arranging a service agreement with an approved service provider to inspect, repair, maintain and, where necessary, upgrade the CCTV recording systems within Trust premises; and to ensure that it is working at its optimum level. The service provider should conduct regular service and maintenance inspections of the CCTV recording system in Trust premises.

5.9 Driving Standards Manager

5.9.1 The Driving Standards Manager (DSM) is responsible for the downloading, viewing, storage and use of any images gathered from the external cameras on any Trust vehicle which has been involved in a road traffic collision (RTC)/Ambulance vehicle incident (AVI), an alleged road traffic incident, or as part of an investigation involving the use of a Trust insured vehicle. It is also the DSM's responsibility to liaise with the Police, insurers or other interested parties if required following such an incident in accordance with section 9 of this policy.

5.9.2 The Driving Standards Manager must also comply with any request from the Information Governance Manager to provide access to relevant persons to view and access CCTV footage within his control.

5.9.3 The Driving Standards manager is also responsible for notifying the Head of Risk and Security and the Information Governance Manager of any significant changes to the external cameras on vehicles.

5.10 Information Governance Manager

5.10.1 The Information Governance Manager is responsible for:

- ensuring that the Trust is registered for the use and operation of close circuit television systems with the Information Commissioner's Office as per the Data Protection Act 2018
- for dealing with requests from Trust Investigators, the Police and members of the public and other Third parties for access to and obtaining images captured by the Trust's CCTV recording systems
- for liaising with the Head of Estates, the Risk Team and the Driving Standards Manager to obtain and view images captured by the Trust's CCTV recording systems.

5.11 Head of Resilience and Specialist Operations

5.11.1 The Head of Resilience and Specialist Operations is responsible for the use, operation, viewing and management of the CCTV recording systems within the Hazardous Area Response Team (HART); and for ensuring that the use of CCTV within HART is carried out in accordance with this policy.

5.12 Senior Education Manager/Driving

5.12.1 The Senior Education Manager/Driving is responsible for:

- ensuring that any footage from driving courses is stored safely and securely and in accordance with this policy
- making any requests to the Driving Standards Manager for the downloading of footage from any of the Driver Education fleet for investigation purposes following a non-driving related investigation/complaint. (CCTV footage would only be shared in accordance with this policy)
- making any requests to the Driving Standards Manager for driving related incidents involving SCAS staff witnessed by the Driving Education Team.

5.13 South Central Fleet Services Ltd

5.13.1 South Central Fleet Services (SCFS) Ltd, under a service level agreement with the Trust, are responsible for:

- the installation, maintenance and repair of the CCTV recording systems in and on Trust vehicles. SCFS Ltd will liaise with the Trust's LSMS to ensure that the installation of the CCTV recording systems in and on vehicles is done in accordance with the specification
- ensuring that operator's manuals are held and are available at each premises where this work is carried out
- ensuring that the images captured and recorded by the CCTV recording systems in and on vehicles are of an appropriate quality
- informing the Trust of any repairs carried out or required to the CCTV recording systems in and on vehicles
- informing and discussing with the Trust's LSMS and the Information Governance Manager any intended changes to the CCTV recording systems in and on vehicles
- ensuring that the inspection, maintenance and repair of the CCTV systems

in and on Trust vehicles is recorded and maintained
- ensuring that these records are made available for inspection and/or audit purposes.
- ensuring that they comply with the Data Protection Act 2018, the General Data Protection Regulation, the CCTV Code of Practice and the Security Industry Licensing requirements.

For further details of the responsibilities of SCFS Ltd, please see Appendix 4.

6. Types of CCTV recording systems in use within the Trust

6.0.1 The Trust has the following Closed circuit television (CCTV) recording systems in place, namely in some Trust premises and in and on Trust vehicles; and also portable and body worn cameras.

6.0.2 The use of CCTV recording systems in the Trust is subject to the requirements of the Data Protection Act 2018 and the General Data Protection Regulation and, as such, needs to comply with Data Protection Principles, see section 11.

6.0.3 The Trust is registered to operate CCTV cameras under the Data Protection Act 2018.

6.1 CCTV recording systems installed at some of the Trust's premises

6.1.1 Some of the Trust's premises have a 24 hour CCTV recording systems installed and where it installed the following is in place:

- appropriate signage will be displayed to inform staff, visitors and the general public that CCTV is in operation
- the CCTV cameras will be sited in such a way that they can only monitor the areas intended to be monitored by the equipment
- the CCTV monitors will be located and access to them controlled so that they can only be accessed and viewed by authorised personnel (see appendix 2).

6.2 CCTV recording systems installed in Trust vehicles

6.2.1 Trust vehicles have CCTV installed in them and there are cameras located on the outside of vehicles (in the front, the rear, nearside and offside of the vehicle) and also in the saloon of the vehicle. The CCTV recording systems consist of a hard drive system, with the SRVs having a flash card system hosted by Vision Unique Equipment (VUE) Ltd.

6.2.2 No audio is captured by external cameras, only the saloon camera captures audio when activated.

6.3 CCTV recording systems used by the Hazardous Area Response Team (HART)

6.3.1 The Hazardous Area Response Team (HART) have fixed and portable CCTV cameras; and staff in HART have body worn cameras. These cameras have the

ability and functionality to stream live images via satellite to Trust locations.

6.3.2 The use, operation, viewing of any images captured by the cameras in operation in HART will be in accordance with this policy.

6.3.3 The HART fleet is equipped with the VUE VDR8 BRX system and footage downloading and use falls under the same rules and regulations as frontline SCAS vehicles.

7. The purpose of the Trust's CCTV recording systems and the use of images captured by these systems

7.1 The Trust's CCTV recording systems and the use of the images captured by these systems are for:

- maintaining the security of premises, vehicles and assets by assisting with the protection of premises, vehicles and assets
- detecting, preventing and investigating incidents of theft of, or damage to, Trust property and assets
- protecting staff and patients or other individuals whose image(s) may be captured
- investigating patient safety concerns and/or the concerns of other individuals whose image(s) may be captured
- investigating incidents involving abuse and threats to Trust staff and others involved in Trust work
- investigating attempted or actual assault of Trust staff and others involved in Trust work in the saloon of Trust vehicles
- investigating road traffic collisions (RTCs)/Ambulance vehicle incidents (AVI) and road traffic incidents/complaints which involve Trust vehicles.

7.1.2 Any information/images captured by the Trust's CCTV recording systems shall only be used for the purposes and means as defined in this policy.

7.1.3 Recorded information/images shall not be sold or used for commercial purposes or the provision of entertainment.

8. CCTV recording systems in the saloons of vehicles

8.0.1 The CCTV recording systems currently installed and working within Trust Ambulances which are linked to the internal cameras in the saloons consist of the following types of systems:

- A hard disk system is installed in the WAS Mercedes vehicles (62-plate onwards) and which, once activated, will record from five seconds before the panic strip is pressed and for the remainder of the recording. The recorded footage is held for three weeks before being overwritten.
- A remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd.

8.1 Activation of the CCTV recording systems in the saloon of Trust vehicles

8.1.1 The CCTV recording system in the saloon of Trust vehicles is activated by pressing the emergency strip located in the ceiling of the saloon; this strip runs from the front to rear of most Trust vehicles. In the WAS Mercedes vehicles the activating strip runs along the ceiling of the vehicle, there is also an activating strip located on the side wall of the vehicle close to the attendant's chair at the head-end of the stretcher.

8.1.2 If a saloon activation of an actual or potential incident has taken place the member of staff who activated the CCTV recording system must contact the Operational Support Desk (OSD). They must also report the incident using the Trust's incident reporting system, Datix.

8.2 Retrieval of images captured by the CCTV recording systems in the saloon of Trust vehicles

8.2.1 Following the reporting of an incident involving the activation of the internal cameras in the saloon of a Trust vehicle, and/or following the retrieval of a request of any images captured, a member of the Risk Team will arrange for the removal of the hard drive and store this in a secure place and/or will retrieve the image from the system supported and managed by Vision Unique Equipment (VUE) Ltd and store in a secure place.

8.2.2 On removal of the hard drive and/or the images from the system supported and managed by Vision Unique Equipment (VUE) Ltd for viewing purposes or for use in legal proceedings, the member of the Risk Team will ensure the following is documented and recorded on the associated incident report form on Datix:

- The date and time of removal
- The reason for removal
- The name of the person removing the hard drive and/or viewing and retrieving the images from the system supported and managed by Vision Unique Equipment (VUE) Ltd
- The name(s) and organisation of the person(s) viewing or receiving the images
- The location of the images and any other relevant information
- The outcome of the viewing
- Any crime unique reference number (URN) to which the images may be relevant
- The signature of the collecting Police Officer
- The date and time the hard drive/flash card was returned to the system or secure place, if they have been retained for evidence purposes.

8.3 CCTV Recording systems on the exteriors of vehicles

8.3.1 The CCTV recording systems currently installed and working and linked to the exterior cameras of Trust vehicles consist of:

- WAS Mercedes double crewed ambulances (62-plate onwards) have front, rear and side facing cameras installed which continuously record, whilst powered up. Recordings will be held on the hard drive for approximately four weeks before being overwritten.

- WAS FIAT DCAs (68 plate onwards) have the same system fitted as above, with the additional facility to remotely carry out a health check on the system and remotely download footage via the hosted system as described in section 8
- Skoda SRVs (68 plate onwards) have the same system and functionality as the WAS FIATS, with the only difference being they only have front and rear cameras fitted and no internal camera.

8.3.2 The recordings of images from external cameras are stored on the same device as the interior saloon cameras. They can also be stored on the system supported and managed by Vision Unique Equipment (VUE) Ltd.

8.4 Activation of the external CCTV cameras on vehicles

8.4.1 Once the ignition on these vehicles is turned on, the external cameras are automatically activated and begin recording after around 30 seconds.

8.4.2 In some Trust vehicles, in addition to the CCTV recording system, an Incident Data Recorder (IDR) is also installed. The Incident Data Recorder will capture the speed of the vehicle, and other electric inputs and the forces acting on the vehicle if the vehicle is involved in a road traffic collision (RTC)/Ambulance vehicle incident (AVI).

8.5 Retrieving information from external cameras following a road traffic incident

8.5.1 As part of the ensuing investigation process following a road traffic collision (RTC)/Ambulance vehicle incident (AVI) and/or road traffic incident/complaint, the following information will be recorded on the specific Driving Standards form (DSD/IDR/IRIS/Download form) and may be included within the Investigation Report if deemed relevant by the Driving Standards Department: See Appendix 6 for Driving Standards form.

- The date and time of removal
- The reason for removal
- The name of the person removing the hard drive or downloading and retrieving the footage from either the hard drive or the computerised system supported and managed by Vision Unique Equipment (VUE) Ltd
- The name(s) and organisation of the person(s) viewing or receiving the images from the hard drive or the computerised system supported and managed by Vision Unique Equipment (VUE) Ltd
- The location of the images and any other relevant information
- The outcome of the viewing
- Any unique crime reference number (URN) to which the images may be relevant
- The signature of the collecting Police Officer
- The date and time the hard drive/flash card was returned to the system or secure place, if they have been retained for evidence purposes.

8.5.2 Where necessary, Driving Standards may share footage from road traffic

incidents/AVI with the Police and/or the Trust's Motor Insurers. This may be done by utilising the computerised system hosted by Vision Unique Equipment (VUE) Ltd.

9. Access to the Trust's CCTV recording systems and recorded images

9.0.1 Access to the Trust's CCTV recording systems and recorded images will only take place in accordance with this policy. Therefore, only authorised personnel as stated in appendix 2 will have access to the CCTV recording systems in Trust vehicles and premises.

9.0.2 Only authorised personnel as stated in appendix 2 will have access recorded images/information from Trust's CCTV recording systems.

9.1 Trust Investigator's requests to view and use CCTV footage

9.1.1 As part of an investigation into an incident, Trust Investigators may request to view and use footage captured by the Trust's CCTV recording systems. When doing this they must make the request in writing to the Trust's Information Governance Manager and must state why they wish to view and use the footage, namely for the investigation of an incident/enquiry/complaint.

9.1.2 Once the request has been received, the Information Governance Manager will liaise with the Head of Estates/the Risk Team/Driving Standards Manager to retrieve the footage from the Trust's CCTV recording systems.

9.2 Police access to images recorded by the Trust's CCTV recording systems

9.2.1 Under the Police and Criminal Evidence Act (PACE) 1984, and the appropriate exemptions of the Data Protection Act 2018, the Police may apply to the Trust for access to hard drives or recorded images taken from the Trust's CCTV recording systems and the computerised system hosted by Vision Unique Equipment (VUE) Ltd, where they reasonably believe that these hard drives/flash cards and/or the said computerised system have captured images that will assist with their investigation and detection of crime and/or the prevention of crime.

9.2.2 All requests for such hard drives/recorded images should be made in writing to the Trust's Information Governance Manager, who would liaise with the Trust's LSMS and/or Driving Standards Manager to retrieve the requested material.

9.2.3 When making the request, the Police should state clearly the purpose of the request and how a failure to disclose the hard drives/recorded images would adversely affect their investigation and prejudice the stated purpose. For example, the request should make clear why it is envisaged that the provision of information would prevent crime and/or why the apprehension or prosecution of an offender is necessary and how the information will assist in the investigation, e.g. why proceedings might fail without the information.

9.2.4 The Trust can share material/images with the Police for the following reasons:

- For the prevention and detection of crime
- The apprehension or prosecution of offenders.

9.2.5 When a request is made by the Police to obtain a copy of the hard drive and/or recording from the computerised system hosted by Vision Unique Equipment (VUE) Ltd, a verified copy of the hard drive and/or recording from this system will be provided to them and the Trust will retain the original hard drive.

9.2.6 The Staff involved in an incident being investigated by the Police may have to provide the Police with statements.

9.3 Requests from the public to access CCTV images

9.3.1 Members of the public are entitled to make requests (subject access requests) under the Data Protection Act 1998 for copies of images of themselves captured and held as a result of the operation/activation of the Trust's CCTV recording systems.

9.3.2 In the event of such a request the member of the public shall be provided with a standard subject access request letter. See appendix 3.

9.3.3 Up until May 2018, the Trust could levy a charge (up to a maximum of £10) to cover the cost of dealing with the request. However, since the General Data Protection Regulation came into force in May 2018, the Trust can no longer levy a charge for dealing with a request for a single copy of images captured and held by the Trust's CCTV recording systems but may be able to charge for multiple or repeat copies.

9.3.4 The Information Governance Manager will be responsible for considering any such requests in accordance with the Data Protection Act 2018, the General Data Protection Regulation and the CCTV Code of Practice issued by the Information Commissioner's Office and in compliance with this policy.

9.3.5 Once the Information Governance Manager has received a request and is satisfied that the request is in order, they will address it accordingly.

9.3.6 The response should be disclosed as soon as reasonably possible. In accordance with the Data Protection Act 2018, the time frame for replying to data protection subject access requests is one month; however the NHS aims to respond within 21 days. This time frame begins from the initial receipt of a valid request and may only be halted if clarification of the request is necessary.

9.3.7 Subject access requests can be refused on a number of grounds; and in particular where to comply with the request may prejudice:

- the prevention or detection of crime
- the apprehension or prosecution of offenders
- a third party's privacy/confidentiality.

9.3.8 The Trust retains the right as Data Controller to make the ultimate decision about the disclosure of images captured by the Trust's CCTV recording systems.

9.3.9 The Data requested by the subject access request can be copied and securely stored so as to ensure it is available within the designated 40 day's timeframe.

9.3.10 Where the requester who made the subject access request wishes to view the images on the Trust's premises, this should be done in a secure location with only the relevant Trust personnel and the requester present.

9.3.11 Where an individual chooses to view images on a Trust premises, only images that clearly identify the subject will to be disclosed in accordance with section 9 above.

9.4 Other Third party access to recorded images/data

9.4.1 Access to CCTV hard drives/recorded images may be obtained in connection with civil disputes by court order or be extended to lawyers acting for defendants or victims in connection with criminal proceedings subject to appropriate consent.

9.4.2 No other access shall be allowed unless approved by the Director of Patient Care and Service Transformation in conjunction with the Information Governance Manager and the Trust's LSMS who will review requests in line with the purpose and objectives of the scheme and in accordance with the policy.

10. Storage, security and maintenance of the recording systems in Trust vehicles

10.0.1 Following retrieval, each hard drive will be secured in a locked cupboard. Any images taken from the remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd system will also be secured safely by the person who retrieved them from the system. This will deter or prevent tampering with or unauthorised viewing of their contents and make any such tampering evident.

10.0.2 Any hard drive or duplicate hard drive which is supplied to an approved third party must be kept in a secure location. Likewise, any images taken from the remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd.

10.0.3 SCFS Ltd have access to two hard drives for maintenance purposes, which they will keep under locked conditions.

10.0.4 When SCFS Ltd remove the hard drive for maintenance purposes they should keep a record of this and share the following details with the Risk Team:

- The date and time of maintenance
- The name of the person carrying out the maintenance
- The reason for the maintenance
- The type of maintenance being carried out.

10.1 Retention of Images captured by the Trust's CCTV recording systems

10.1.1 CCTV images should be stored and treated in the same manner with the same security and confidentiality of electronic and manual records. CCTV images should be stored within a lockable cupboard to prevent unauthorised access. Likewise, any CCTV images retrieved from the remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd should be stored safely to prevent unauthorised access.

10.1.2 Once images are no longer required, they should be deleted (i.e. images should not be stored any longer than is necessary for a criminal case or investigation to be completed etc.)

10.1.3 Images captured by the Trust's CCTV recording systems should not be retained (even on computers) for more than 31 days, unless this image is part of an investigation (Police or Trust). The Trust must ensure that images are stored in a secure manner to ensure that the images are not corrupted, deleted, misplaced etc.

10.1.4 If images are required as part of an investigation, the images should be secured.

10.1.5 Where images are required to be destroyed the following should take place:

- Hard Drives which have automatic overwriting facilities should be activated so that the material/images is removed;
- Images that have been printed off as a still shot, should be shredded and disposed of in confidential manner;
- CCTV that has been put onto a disc should be shredded using a shredder that has the facilities for this;
- CCTV images retrieved from the remote hosted system supported and managed by Vision Unique Equipment (VUE) Ltd should be deleted from the computer of the person who has retrieved them.
- Driving Standards may need to retain footage relating to a road traffic collision or AVI in cases where a claim may be disputed. This footage would not contain any personal identifiable information within it. Footage would be deleted once the claim was settled, the internal investigation had been completed or it had been shared with insurers.

10.2 Removal of CCTV recording systems

10.2.1 When the CCTV recording systems in a Trust premises or vehicle are obsolete and it is being dismantled and removed then in accordance with the Data Protection Act 2018, the hard drives of these systems must be removed by SCFS Ltd and passed to Driving Standards who will reformat the hard drive and re-use it.

10.2.2 For the CCTV systems in Trust premises, this must be done by the Head of Estates; and for the CCTV systems in Trust vehicles this must be done by the Risk Team.

11. CCTV Signage at Trust premises and in Trust vehicles

11.0.1 To assist with the Trust in complying with the Data Protection Act 2018, appropriate signage informing the public that CCTV is in operation shall be displayed at those Trust premises and vehicles where CCTV recording systems have been installed.

11.0.2 The signage will be displayed on the external façade of Trust buildings and/or at the perimeter of the area covered by the CCTV. The signage will state display details of the organisation who is operating the system, namely, the South Central Ambulance Service NHS Foundation Trust. It should also display the contact details for any enquires or complaints.

11.0.3 There will also be a sufficient number of signs and it will be positioned so that, so far as reasonably possible, that individuals entering the area covered by CCTV will be aware of the presence of CCTV and that CCTV is in operation.

11.0.4 Appropriate signage will also be installed in the saloon of the vehicle.

11.0.5 There is no requirement to place signs directly under cameras.

12. Compliance with the principles of the Data Protection Act, the General Data Protection Regulation and offences under the DPA

12.1 The Trust has to comply with the principles of the Data Protection Act 2018 which are that personal information shall:

- be fairly and lawfully processed
- be collected for specified, explicit and legitimate purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be kept for longer than is necessary
- be processed in accordance with the data subject's rights, and in a manner that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical/organisational measures
- not to be transferred to countries without adequate protection.

12.2 Failure to comply with the above can result in the Trust being fined.

12.3 The Data Protection Act 2018 also provides for corporate and personal liability for offences under the Act/legislation.

13. Use of CCTV images in connection with disciplinary or capability procedure

13.1 The information/images captured by the Trust's CCTV recording systems may only be used for the purposes as described in section 7 and may not be used against any staff member in any disciplinary and/or capability hearing unless in connection with the use as outlined in section 7.

13.2 If the information/images captured by the Trust's CCTV recording systems are to be used in connection with any disciplinary and/or capability procedure and/or any investigation/complaint involving a member of staff then the member of staff has the right to request and view the information/images captured by the CCTV.

14. Use of CCTV images in connection with Clinical negligence

14.1 The information/images captured by the CCTV recording system may only be used for the purposes as described in section 7 and may not be used against any staff member in any allegation of clinical negligence unless in connection with the use as outlined in section 7.

14.2 If the information/images captured by the Trust's CCTV recording systems are to be used in connection with any clinical negligence and/or any investigation/complaint involving a member of staff then the member of staff has the right to request and view the

information/images captured by the CCTV.

15. Staff being filmed by Members of the Public (MOP) in a public place

15.1 There is no legislation to prevent a member of the public from filming anyone in a public place and this includes members of the public filming Trust employees. Trust employees, however, can object to being filmed and can ask in a polite way for the member of the public to stop filming them. If a member of the public does not comply with this request then the Trust employee can report the matter using the Trust's incident reporting system, Datix.

15.2 There is legislation to prevent a member of the public filming a Trust employee if they are on Trust premises. If this happens then the Trust employee should report the matter using the Trust's incident reporting system, Datix. They should also report the matter to the police as the police have the power under S 43 of the Terrorism Act 2000 to stop, examine and seize any recorded material.

16. Body Worn Cameras Pilot

16.1 The Trust has secured funding from NHS England and NHS Improvement to undertake a body worn cameras pilot in 2021. It is intended that this pilot will commence in May 2021 and be 12 months in duration.

16.2 At the end of the pilot, NHS England and NHS Improvement will have it independently evaluated and the results of the evaluation will be shared with Ambulance Trusts so that they can decide whether to continue with the use and operation of body worn cameras.

16.3 The body worn cameras will be supplied by Motorola and this company will also manage and control the UK based computerised system (i-cloud) for the recording and storage of any recording.

16.4 The use and operation of body worn cameras will be operated in accordance with this policy and the relevant legislation such as the Data Protection Act 2018 and the General Data Protection Regulation.

16.5 In accordance with this policy and its principles, only authorised Trust personnel will have access to any downloads and the viewing of them.

16.6 It is intended that the body worn cameras will be issued to those frontline 999 Operational Resource Centres where staff have reported the highest number of violence and aggression incidents.

16.7 Staff who take part in the pilot will be trained in the safe use and operation of the body worn cameras; and only these staff will be able to use and operate the body worn cameras.

16.8 It will be up to the staff issued with the cameras to decide when they will switch them on and start recording.

16.9 Once the body worn cameras are switched on, they will record images and audio.

16.10 Recorded Material is encrypted to protect it the equipment is lost, stolen or breached.

16.11 The body worn cameras system does not have facial recognition or other biometric characteristic recognition capabilities.

16.12 The use and operation of body worn cameras will be supported by a standard operational procedure which will be shared with all relevant staff before the pilot commences.

17. Training

17.1 All employees are to be informed of this policy during induction. Specific information/training will be given where and when required.

17.2 Training in the use and retrieving of CCTV images will be given when required.

17.3 Training by CCTV system engineers will also be provided as appropriate.

18. Equality and Diversity

18.1 An equality and diversity impact assessment has been carried out on this policy.

19. Monitoring

19.1 The effectiveness of this policy will be monitored regularly.

20. Consultation and Review

20.1 A consultation exercise on the policy will be carried out with the relevant stakeholders

20.2 A consultation exercise on the policy will be carried out with the relevant stakeholders and will be reviewed every three years or sooner if there are any relevant changes to legislation or best practice.

21. Implementation (including raising awareness)

21.1 The policy will be implemented and communicated to managers and staff within the Trust via the weekly newsletter, *Staff Matters*.

22. References

- Health and Safety at Work etc. Act 1974
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- Criminal Procedure and Investigations Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 2018

- General Data Protection Regulation 2018
- Investigatory Powers Act (2016)
- Freedom of Information Act 2000
- Home Office CCTV Operational Requirements Manual 2009
- Home Office Surveillance Camera Code of Practice 2013
- Home Office UK Police requirements for digital CCTV systems
- Information Commissioners Office (ICO) In the picture: A data protection code of practice for surveillance cameras and personal information 2014
- Data Protection (Assessments Notices) (Designation of National Health Service Bodies) Order 2014
- Information Commissioners Office (ICO) Privacy Impact Assessment (PIA)
- NHS Protect Closed Circuit Television
- Surveillance Camera Commissioner Code of Practice: A guide to the 12 principles of surveillance
- Secretary of State's Directions on Security Management Measures (March 2004).

23. Associated documentation

- Health and safety policy and procedures
- Adverse incident reporting and investigation policy
- Security policy
- Violence and aggression policy
- Lone working policy
- Driving and care of Trust vehicles policy
- Discipline and conduct policy.

Appendix 1: Review Table

This policy is regularly reviewed and updated with information in line with relevant national guidance and legislation.

A full ‘Review Table of Contents’ is available on request.

Appendix 2: Authorised Persons to Access or Maintain CCTV Systems

The following persons have been authorised by the Trust to access or maintain the Trust's CCTV systems:

- Director of Patient Care and Service Transformation
- Head of Risk & Security (LSMS)
- Information Governance Manager
- Health, Safety and Security Officer
- Risk Assistant (Clinical)
- Assistant Director of Support Services
- Head of Estates
- Vehicle Commissioning Unit Team Lead
- Driving Standards Manager
- Assistant Driving Standards Assistant
- Motor Claims Lead
- Temporary access may be given to other members of staff or contractors authorised by the Director of Patient Care and Service Transformation or South Central Fleet Services Ltd.

Appendix 3: CCTV Subject Access Information
(Draft letter)

Under the terms of the Data Protection Act 2018, individuals whose images are recorded on CCTV systems have the right to view the images of themselves and unless agreed otherwise to be provided with a copy of those images.

Your attention is drawn to the South Central Ambulance Service NHS Foundation Trust CCTV Policy document, which is available upon request.

The South Central Ambulance Service NHS Foundation Trust will accept requests made for Personal Data under the Data Protection Act. Such requests may be made in writing to the Trust. All requests for personal images contained on CCTV must include:

- The date the image was recorded
- The time the image was recorded
- A recent photograph of the individual captured on CCTV to enable identification
- A description of the clothing worn at the time of the recording
- A description of the scene where the recording took place i.e. vehicle, Trust building

All requests will be dealt with in accordance with the Data Protection Act 2018 and guidance issued by the Information Commissioner's Office in relation to CCTV. This guidance can be viewed at www.ico.gov.uk.

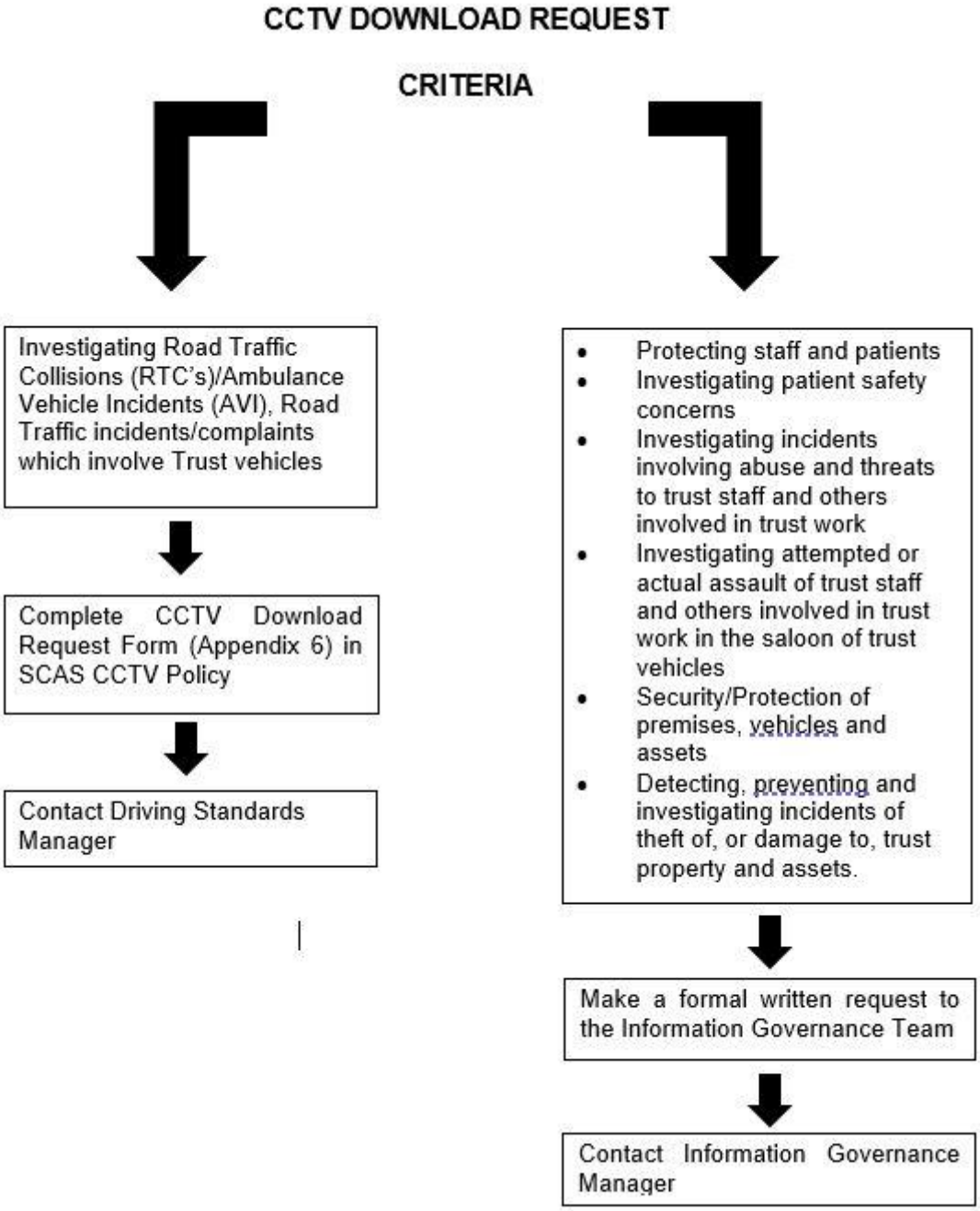
It should be noted that images captured on the Trust's CCTV system are not normally retained for longer than 40 days.

You are reminded that the Trust may not be able to locate your images.

Any request will receive an initial reply within one month.

For further information please ask for a copy of the South Central Ambulance Service NHS Foundation Trust CCTV policy or contact the Trust Information Governance Manager.

Appendix 4: Requesting a CCTV Download



Appendix 5: The Current Agreement between SCAS and SCFS Ltd with regards to Servicing and Maintenance of the VDR8 System

South Central Fleet Services (SCFS) Ltd will:

- ensure that inspection holes are drilled into the BH2 cupboard doors on all Trust vehicles fitted with the VDR8 BRX system. This allows sight of the tell-tale lights that indicate the health of the unit.
- ensure that all DCAs from 68 plate onwards are fitted with the VDR8 CRX system and the driver's tell-tale lights on the dashboard.
- ensure that all SRVs from 68 plate onwards are fitted with the VUE 2 camera system and the driver's tell-tale lights on the dashboard
- supply and fit advisory stickers to the outside of the BH2 locker door to advise basic information around what the lights are indicating.
- check VDR8 units on DCA's at eight week intervals and record when completed within the vehicle's maintenance history.
- check VDR8 units on SRV's at 12 week intervals and record when completed within the vehicle's maintenance history.
- Where a fault has been identified with the VDR8 unit, SCFS Ltd CCTV trained staff will attempt to investigate further and where possible affect a repair
- Where a fault cannot be addressed as within the above, SCFS Ltd Workshops will inform the Vehicle Commissioning Manager, who will investigate further and where possible will attempt to affect a repair / replacement as necessary.
- Faults that cannot be rectified successfully by SCFS Ltd trained staff will be passed to VUE for investigation / resolution.
- Vehicles that have been identified as having a defective or faulty CCTV unit on board will be treated as an absolute priority to either repair or replace the defective / faulty unit.
- Whilst the CCTV units are a vitally important device to assist with the safety of staff and patients, if a CCTV unit is defective or faulty then this is not a reason on its own to remove an otherwise fully functioning Ambulance or sole response vehicle from operational duties.

Appendix 6: Driving Standards Department Form

Many of our policies have an 'Internal staff form' attached that is relevant to the document. The 'Driving Standards Department' form is included with this policy but for security and accessibility reasons it is only available on our Staff Intranet.

Appendix 7: Responsibility Matrix – Policies, Procedures and Strategies

A full responsibility matrix for this policy is available on request.

Appendix 8: Equality Impact Assessment Form Section One – Screening

A full Equality Impact Assessment has been carried out on this policy and is available on request to the public and internally via our Staff Intranet.

Appendix 9: Equality Impact Assessment Form Section Two – Full Assessment

A full Equality Impact Assessment has been carried out on this policy and is available on request to the public and internally via our Staff Intranet.

Appendix 10: Ratification Checklist

A Ratification Checklist for this policy is available on request.