VEHICLE CLOSED CIRCUIT TELEVISION POLICY AND CODE OF PRACTICE

DATE APPROVED: 28 October 2015
APPROVED BY: Trust Board
IMPLEMENTATION DATE: 02 December 2015
REVIEW DATE: February 2017
LEAD DIRECTOR: Emergency Services Director
IMPACT ASSESSMENT STATEMENT: No adverse impact on Equality or Diversity

Document Reference Number: OPS – Policy – 018 (Version 1.1)
## Change Control:

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Document</th>
<th>Version</th>
<th>Owner</th>
<th>All Trust</th>
<th>Issue Date</th>
<th>Next Review Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPS – Policy - 018</td>
<td>Vehicle CCTV Policy and Code of Practice</td>
<td>1.1</td>
<td>Emergency Services Director</td>
<td>All Trust Employees</td>
<td>02 December 2015</td>
<td>February 2017</td>
<td>Head of Safety and Security</td>
</tr>
</tbody>
</table>

## Change History:

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>Comment/Approved by</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 April 2015</td>
<td>Present made to Group by Fleet Manager</td>
<td>RPF</td>
</tr>
<tr>
<td>June 2015</td>
<td>Draft</td>
<td>Head of Safety &amp; Security</td>
</tr>
<tr>
<td>02 July 2015</td>
<td>Details of what has changed/reviewed</td>
<td>TU Policy Group – comments made</td>
</tr>
<tr>
<td>06 July 2015</td>
<td>Suggested changes circulated – Group suggested more changes</td>
<td>TU Policy Group</td>
</tr>
<tr>
<td>14 July 2015</td>
<td>Suggested changes made including having separate policies for vehicle and property CCTV</td>
<td>TU Policy Group – for info</td>
</tr>
<tr>
<td>04 August 2015</td>
<td>Sent for discussion and agreement</td>
<td>OMB – agreed</td>
</tr>
<tr>
<td>18 August 2015</td>
<td>Sent for discussion and agreement</td>
<td>EMB – Agreed</td>
</tr>
<tr>
<td>10 September 2015</td>
<td>Further suggestions received and amended document. Circulated to group</td>
<td>Policy Group – comments made</td>
</tr>
<tr>
<td>21 September 2015</td>
<td>Further suggestions received and amended document. Circulated to Group</td>
<td>Policy Group – comments made</td>
</tr>
<tr>
<td>28 October 2015</td>
<td>Sent for discussion, agreement and ratification</td>
<td>Trust Board</td>
</tr>
<tr>
<td>29 October 2015</td>
<td>Sent for discussion</td>
<td>RPF</td>
</tr>
<tr>
<td>04 November 2015</td>
<td>Sent for discussion – further comments and changes made.</td>
<td>Policy Group</td>
</tr>
<tr>
<td>20 November 2015</td>
<td>Changes to policy made following legal advice from trust solicitors.</td>
<td>Head of Safety &amp; Security</td>
</tr>
<tr>
<td>02 December 2015</td>
<td>Group agreed to document subject to review in 6 months.</td>
<td>Policy Group</td>
</tr>
<tr>
<td>15 November 2016</td>
<td>Negotiations ongoing, agreed to extend current policy with short review date.</td>
<td>Policy Group</td>
</tr>
</tbody>
</table>
CONTENTS

1 Introduction .............................................................................................................................................. 4
2 Aim ............................................................................................................................................................ 4
3 Objectives of the CCTV Scheme ........................................................................................................... 6
4 Statement of Intent .................................................................................................................................. 6
5 Responsibilities ......................................................................................................................................... 7
6 Operation of the System .......................................................................................................................... 8
7 Definition of WMAS CCTV/DVR System ............................................................................................... 8
8 Vehicle Procedures, Normal Operation & Recording Process .............................................................. 9
9 Activated Recordings – Saloon Area of Vehicle ...................................................................................... 10
10 External Incidents .................................................................................................................................. 11
11 Retrieval & Storage of Incident Recordings from Ambulance CCTV Systems ...................................... 11
12 Access/Review Procedure ....................................................................................................................... 12
13 Police Access ......................................................................................................................................... 12
14 Third Party Access ................................................................................................................................. 12
15 Subject Access Requests ....................................................................................................................... 13
16 Signage .................................................................................................................................................... 14
17 Maintenance .......................................................................................................................................... 14
18 Fault Reporting ..................................................................................................................................... 15
19 Quality of Images .................................................................................................................................. 15
20 Disciplinary Procedure ........................................................................................................................... 15
21 Complaints ............................................................................................................................................ 15
22 Breaches of this Policy ........................................................................................................................... 15
Annex A - Correspondence Template for Subject Access Request ......................................................... 16
Annex B Subject Access Request Form ...................................................................................................... 17
Annex C Footage Review Access Log ....................................................................................................... 20
Annex D Footage Retention Log ............................................................................................................... 21
Annex E Photographic/Image Printing Log .............................................................................................. 22
Annex F Genisys Display Panel ................................................................................................................ 23
Annex G Incident Download Log .............................................................................................................. 24
Annex H Maintenance Procedure Manual/Footage Retrieval ................................................................. 25
1 Introduction

1.1 The purpose of this Code of Practice is to regulate the management, operation and use of the closed circuit television (CCTV) system within all West Midlands Ambulance Service vehicles which have the equipment installed.

1.2 The systems in each vehicle will comprise of a number of fixed and dome cameras located around the site/vehicle site. All cameras are monitored/recorded from a controlled/restricted location/housing and are only available for view/preview to selected staff and managers.

1.3 This Code of Practice follows Data Protection Act guidelines. The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.4 The CCTV system is owned by West Midlands Ambulance Service NHS Trust and as such is registered with the Information Commissioners Office as follows:

Registration Number: ****************
Date Registered: ****************
Registration Expires: ****************
Data Controller: ****************
Address: West Midlands Ambulance NHS Foundation Trust, Waterfront Business Park, Waterfront Way, Brierley Hill DY5 1LX

2 Aim

2.1 The purpose of this policy is to explain the operational use of Trust vehicle mounted Closed Circuit TV (CCTV) recording system. The Trust’s CCTV recording system(s) is for preventing and investigating crime, protecting staff and accurately investigating road traffic collisions involving West Midlands Ambulance Service vehicles.

2.2 To contribute to the protection of people and property with an emphasis on people first.

2.3 It is our aim to protect staff safety and welfare and to reduce the overall level of crime (theft, fraud, property/vehicle damage, violence) which effects West Midlands Ambulance Service and its stakeholders and also improve employee and public perceptions of their safety and security within West Midlands Ambulance Service.
2.4 In pursuit of this aim, West Midlands Ambulance Service will:
Ensure that all employees operating the CCTV system are appropriately trained, accredited, and vetted.

1. Ensure that the system is operated in accordance with the Data Protection Act (1998) and its associated guidance and ACOP (approved code of practice).
2. Ensure that proper management and control procedures are in place to protect the integrity and security of all recordings made using the CCTV system.
3. The CCTV system installed in operational vehicles is not to be used in relation to “Patient Treatment” issues. It is there for the detection of crime / assaults against trust staff.
4. A copy of the Fleet Services “Maintenance Procedure Manual/Footage Retrieval is attached appendix “H”

2.5 This policy details the circumstances when the CCTV recording system may be used by West Midlands Ambulance Service NHS Foundation Trust or by external agencies such as the Police in connection with any alleged incident connected with the following:

The detection, prevention or reduction of incidents of theft from trust vehicles, alleged incidents of violence against Trust employees or any person or persons involved in Trust work, or to ascertain the actual events leading up to, during and following a road traffic collision involving a West Midlands Ambulance Service vehicle

2.6 This policy will explain when a recording may not be used, for example as part of any disciplinary procedure or in connection with any alleged clinical negligence against a member of staff, sickness or capability issues.

2.7 The use of CCTV recording systems is subject to the requirements of the Data Protection Act 1998 and as such needs to comply with Data Protection Principles. The Trust is registered to operate CCTV cameras under the Data Protection Act.

2.8 This policy has been written to safeguard the individual’s rights in compliance with the relevant legislation and guidance including: Health & Safety at Work Act 1974; Human Rights Act 1998; Secretary of State Directions to NHS bodies in particular “Security Management measures” (March 2004); Guidance issued by the NHS Counter Fraud and Security Management Service (CFSMS), relating to CCTV; Guidance issued by the Information Commissioner’s Office, and Guidance issued by the Security Industry Authority.

2.9 The planning, design and approval of the vehicle CCTV system has endeavoured to ensure that the system will be give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the general area of coverage.
3 Objectives of the CCTV Scheme

3.1 This policy applies to all trust staff or any other persons employed directly or indirectly by the Trust who are involved in patient care / treatment or any other dealings with any member of the public within Trust property or the saloon area of emergency response vehicle fitted with a CCTV recording system, or any persons driving a Trust vehicle in the case of an road traffic collision activation. Once activated the CCTV system will record audio as well as images within the saloon area of operational vehicles but **NOT** within the cab area.

3.2 This policy confirms that the Trust will not utilise any audio recording device within the cab area of operational vehicle. In addition to this, no member of staff has authorisation to access any devices for the purpose of ambient listening. The only exception to this statement is subject to the ARP Ambient Listening Policy (IM&T – Policy – 014).

3.3 Any information captured by the CCTV recording system shall only be used for the purposes of:

1) To increase personal safety and reduce the fear of crime
2) Protecting the trust sites, vehicles and its assets.
3) To assist in identifying, apprehending and prosecuting offenders of criminal damage.
4) To protect members of the public and private property
5) To support the Police in a bid to deter crime.

3.4 Any information captured by the CCTV recording system shall only be used for the purposes as defined in this policy and by the means as described in this policy (Section 3.2).

3.5 Access to recorded material shall only take place as defined in this policy as detailed in section 11.

3.6 Recorded material shall not be sold or used for commercial purposes or the provision of entertainment

3.7 The showing of recorded material shall only be released in accordance with the law, either in compliance with the needs of the police in connection with the investigation of crime, which shall be conducted in accordance with the provision of any relevant policy under the Police and Criminal Evidence Act 1984 and any advice and guidance given to the police from time to time, or in any other circumstances provided by law.

4 Statement of Intent

4.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner’s Code of Practice.
4.2 The Trust will treat the systems and all information, documents and recordings obtained and used as data which are protected by the Act.

4.3 Materials, footage, or intelligence secured as a result of CCTV will not be used for any personal use by stakeholders. Footage will only be released to the media for use in the investigation of a specific crime and with the written authority from both the West Midlands Ambulance Information Governance Manager based at Millennium Point Headquarters. Any staff members visible on the footage and of the Police Footage will never be released to the media for purposes of entertainment. (6 month audit to be presented to RPF group.)

4.6 Information signs, as required by the Code of Practice of the Information Commissioner will be placed at all access routes to areas covered by the site and vehicle CCTV system.

5 Responsibilities

5.1 The Director of Corporate Services, as the Security Management Director (SMD), has overall legal responsibility for the Trust’s CCTV system(s).

5.2 The Trust’s Director of Service Delivery, Head of Fleet Services and LSMS (Local Security Management Specialist) is responsible for maintaining an oversight of the CCTV systems, and the procedures supporting their operational use, to ensure compliance with NHS Security Management Service guidance and provide assurance to the SMD that the requirements set out in that guidance are met.

5.3 The Head of Fleet Services (Or Deputy) and/or the LSMS is responsible for the retrieval, downloading, storage and use of any images gathered from a vehicle which has been involved in a road traffic collision or where a member of staff has activated the internal vehicle recording system. It is the staff member involved in such incidents responsibility to advise the EOC, it is the EOC Duty Manager responsibility to advise the Head of Fleet & LSMS that an incident has occurred and the retrieval of footage may be necessary.

5.4 The Fleet Manager shall be responsible for the installation and maintenance of the CCTV recording system within vehicles. Ensuring that the images captured and recorded by the system are of an appropriate quality; and, that logs of inspection, maintenance and repair work in respect of the CCTV system are properly maintained and audited.

5.5 The Trusts LSMS and Head of Fleet Services shall be responsible for maintaining secure access to all recordings which may be captured by the CCTV recording system on the system’s removable recording media. The post holders shall be responsible for the removal of any hard disk following any incident and for the installation of a replacement hard disk.
5.6 The Fleet department shall be responsible for the day to day maintenance and servicing of the CCTV recording system on all vehicles. This will be undertaken during routine servicing/safety checks.

5.7 All staff involved in the operation of CCTV or the monitoring of images have a responsibility to comply with the provisions of the Data Protection Act 1998, CCTV Code of Practice and Security Industry Authority Licensing requirements. Any breaches of this policy by staff involved in the operation of the trust CCTV system may/will be subject to the Disciplinary Policy/procedure.

6 Operation of the System

6.1 The systems will be administered and managed by the Trust’s Head of Information and Governance, in accordance with the principles and objectives expressed in this policy.

6.2 The overall responsibility to ensure that the Trust adheres to this Code of Practice lies with the West Midlands Ambulance Service Head of Information and Governance based at Millennium Point Headquarters.

6.3 The day-to-day management will be the responsibility of both the Trust’s Local Security Management Specialist and the Fleet Manager.

6.4 The vehicle CCTV system should be operational 24 hours a day, every day of the year. If the whole or part of the system is inoperable then this should be fixed without delay and if necessary escalated to the Head of Fleet services who will expedite rectification actions. Should the CCTV system be faulty it will be rectified as a matter of priority. Where CCTV is fitted/activated, and reported faulty the vehicle will be withdrawn from operational duties and only used when other operational vehicles are not available.

7 Definition of WMAS CCTV/DVR System

7.1 CCTV referenced within this policy refers to the monitoring, recording equipment Operated within front line operational vehicles and on trust sites.

7.2 Depending on the vehicle model and year the equipment consists of: An Active Digital Video Recorder (DVR), storing data on numbered, SD Cards or Vehicle based Hard Drives and locked in a secure compartment within the vehicle.
• Cameras positions on a DMA are:

The vehicle contains two display screens (One in the front cab and one in the rear saloon, dependant on vehicle age/ type. Latest vehicle have a single display screen in the rear saloon)
  o Discreet internal dome camera mounted on the internal roof panel in the rear saloon (Some vehicles will have 2 rear saloon cameras dependant on vehicle age/ type)
  o 1 x front facing camera mounted on the windscreen
  o 2 x side mounted cameras facing towards the front of the vehicle (Dependant on vehicle age and CCTV specification)
  o 1 x rear facing camera mounted in the number plate holder

• Camera Positions on an RRV are:

  o 1 x front facing camera mounted on the windscreen
  1 x rear facing camera mounted in the number plate holder

8 Vehicle Procedures, Normal Operation & Recording Process

Normal Operation

8.1 The CCTV recording system is operated via the vehicles communications system which has an independent battery supply and not subject to a ‘Time Out’ period. The external cameras will continue to operate whilst the vehicle is operational / on run lock indefinitely however, once the ignition is switched off completely the external cameras will only operate for 30 minutes and then shutdown.

8.2 For all cameras EXCEPT the Saloon camera the CCTV system is active and recording whilst the ignition is switched on – the CCTV stops recording 30 minutes after ignition is switched off.

8.3 The saloon camera passively records on 30 second loops. On activation of the saloon camera the CCTV hard drive will write the passively recorded footage from 30 seconds prior to activation and continue to record until Switched off by the crew. Saloon camera footage is not viewable in any way unless it has been activated by the crew.

8.4 The rear saloon display screen will normally present all the external cameras views on rotation. View from the rear saloon mounted camera(s) will only be displayed when the recording facility is activated. ((Displays subject to vehicle age/ system installed)
9 Activated Recordings – Saloon Area of Vehicle

9.1 The CCTV recording system is activated by either pressing the emergency “Attendant Strips” or the CCTV activation button on the Genesis panel located in the rear saloon. The RED strip runs from back to front. Once activated the CCTV recording function can only be stopped from the Operators switch panel in the front cab. (Appendix “F”)

9.2 Once activated via the RED strip an audible warning will be given indicating visual and audio recording is ongoing. This audio message will repeat periodically in the saloon area. Alternatively the system can be activated via the CCTV button on the genesis panel being pressed. When activated via this route no audio warning will be given.

9.3 Upon activation, SD Card or Vehicle based Hard Drive within the CCTV DVR will record the live video and audio stream from the saloon area of the ambulance and continue to record until the CCTV recording facility is deactivated via the front cab operator’s switch. The system, on activation will automatically convert the previous 30 seconds into live mode which will form part of the evidence file, showing the immediate incident prior to activation. (NOTE Vehicles fitted with SD card media upon activation will record the saloon area of the vehicle for 240 seconds and then automatically deactivate. If further recording is required the activation strip/button must be pressed again for a further 240 seconds etc. As SD cards are replaced by hard drives re-activation will not be required.)

9.4 Additionally, upon activation an audio warning will commence indicating to all occupants within the ambulance that video and audio recording is in progress. This message will repeat itself until the recording is deactivated. This message does not sound if the system is activated by the Genesis panel.

9.5 Deactivation should commence once the incident has been concluded, (i.e. patient discharged from vehicle) or other external agencies take over (police etc.).

9.6 All recordings are encrypted and time stamped, so as to be admissible evidence in court.

9.7 Once the CCTV recording has been activated and the incident has been concluded the Crew must inform the EOC Duty Manager (DM) via whatever means is practical. The DM will then contact the Fleet department who will arrange for the immediate removal and Storage of the recording and replacement of the SD Card or Hard Drive data. **This action will be completed within 12 hours to preserve the recordings as retrieval is time critical to prevent the image being recorded over as the system loops**

9.8 The staff members affected by the incident must be allocated time to report the incident via the trust WMAS 54 and advise the EOC that they activated the CCTV recording system on this incident.
9.9 The CCTV system in the rear saloon is there for preventing / investigating crime and protecting staff from assault. System activation is controlled by the clinicians on scene and consideration of such an activation should be undertaken on the basis of an actual assault or perceived threat from the patients or others on board the vehicle.

10 External Incidents

10.1 This policy covers the operational use of the vehicles front, side and rear facing CCTV recording facility.

10.2 The CCTV recording system is operated from the vehicle ignition system and automatically powers down 30 minutes after the vehicle ignition is switched off. The CCTV system automatically powers up on activation of the vehicle’s ignition.

10.3 The digital recorder is installed in a locked cabinet within the vehicle; the cabinet is fitted with a specific security locking system to which only authorised personnel have access. All data is recorded in a proprietary format and cannot be viewed without the relevant software which is only issued to authorised personnel. Removal of SD cards is logged into the memory of the DVR unit and is tagged with a time and date.

10.4 Any security keys issued to authorized personnel must be kept in safe and secure locations.

11 Retrieval & Storage of Incident Recordings from Ambulance CCTV Systems

11.1 The CCTV systems records onto a SD Card or Vehicle based Hard Drive. Once the recording function has been activated, all video and audio of any incident occurring externally and in the rear saloon will be stored on the SD Card or Vehicle based Hard Drive in the CCTV unit in the ambulance. The recordings are encrypted and cannot downloaded or viewed by unauthorised persons.

11.2 Following conclusion of the incident, the Fleet Manager, his deputy and/or the LSMS will respond to retrieve and replace the relevant hard drive/ memory card. Appropriate tools & replacement memory cards will be carried by them at all times. Once removed, the Fleet Manager/LSMS will complete a statement detailing the removal and retention in a legally acceptable format pending Police involvement. (Appendix “G”).

11.3 The Fleet Manager/LSMS will then complete the incident form or report which will facilitate the completion of relevant information as detailed below. In doing so it is essential that the following details are completed on the form;
• The date & time which the information was removed from the vehicle
• Identity numbers of the cards removed/replaced
• The vehicle registration number and unique WMAS fleet number
• CAD log number
• Staff names & Operational base station involved in this incident
• Any general information applicable to the incident.
• Details of Police Officers attending, particularly where the evidential SD card or Vehicle based hard drive data is provided to them as part of their prosecution case. This is vital to ensure we can evidence a complete chain of custody for the evidence

12 Access/Review Procedure

12.1 The Fleet Managers/LSMS will be the authorised persons who will have the access rights to review the encrypted footage.

12.2 All recorded material not retained by the Police will be stored in line with Trust Policy and the national guidance for a minimum of 12 months within a secure folder on the WMAS network. (Appendix C &D). The trust will retain a copy of all data passed to the Police for a period of 12 months or until the case has passed through the criminal justice system.

13 Police Access

13.1 Police may obtain access to the footage under the provision of the Police and Criminal Evidence Act 1984 (PACE). Police requests for access should be made in writing to the Trust utilising the recognised Data Protection Act (DPA) form and should state that the purpose of the request and, as clearly as possible, how failure to disclose would prejudice the stated purpose. The form then must contain the physical signature of the requestor, the countersignature of a sergeant or above and then passed to the Data Protection Officer for processing. Where a request for data is received from the police and released, the staff involved in the investigation will be notified of this request as a matter of courtesy.

13.2 Where there is the need to expedite this process so as to support a prosecution case of violence and aggression towards WMAS staff, the Fleet Manager/LSMS will provide with the footage together with the statement, in lieu of actual receipt of the written DPA request.

14 Third Party Access

14.1 Access to the imagery contained on Trust systems may be obtained in connection with civil disputes by court order, e.g. protests, riots etc., or to be extended to lawyers acting for Trust staff in connection with civil / criminal proceedings or following a RTC.
Trust staff may request specific recordings / photographic images in circumstances where they intend to take out a private prosecution. Approval for release (where retained) must be obtained from the Director of Operations / SMD (Appendix E).

Where a request for data is received from the police etc. and released, the staff involved in the investigation will be notified of this request as a matter of courtesy

15 Subject Access Requests

15.1 Under the Data Protection Act 1998, an individual has the right to view any personal information held about them by an organisation. All requests should be made in writing via the Data Protection Officer with two recent forms of identification i.e. passport or driving licence to confirm the identity of the requestor and a recent utility bill to confirm the correct postal address for the individual to return any correspondence to (Appendix A). A consent form must also be signed by the individual. This can be obtained from the Data Protection Officer. (Appendix B).

15.2 All Subject Access requests must be directed to Data Protection Officer and as per the Data Protection Act, they will be responded to within forty calendar days (40 days) of receipt of the request. Unless the Data Protection Officer has received a request in writing, and received supporting evidence (preferably photographic) in order to identify the subject, then they do not need to comply with the request. It is recommended that the Data requested by the Subject is copied and securely stored in order to ensure its availability within the 40 days.

15.3 Unfortunately the request for information that West Midlands Ambulance Service holds on a Data Subject is sometimes requested for no reason other than to cause disruption to the Trust’s operation. Therefore the Information Governance Manager does not need to comply with a Subject Access request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed. West Midlands Ambulance Service considers this reasonable time lapse to be three months (3 months) or more unless there has been another incident.

15.4 Requests for Subject Access may be refused on a number of grounds; in particular there are exemptions to subject access rights where to comply with the request may prejudice:
   a) The prevention or detection of crime, or
   b) The apprehension or prosecution of offenders

15.5 If the data subject wishes to view the images on site, as opposed to a copy being sent, then this service must be offered to the subject and the viewing should take place in a closed office with only the relevant individuals present, but no fee will be levied against the subject for this request.
15.6 The Trust retains the right as data controller to make the ultimate decision on disclosure of CCTV images in respect of subject access requests and does so on the understanding that it considers if it may / will prejudice the prevention or detection of crime, or the apprehension or prosecution of offenders.

16 Signage

16.1 Signs should be placed so that the public and employees are aware that they are entering a zone which is covered by surveillance equipment. The signs should be clearly visible and legible to members of the public.

16.2 The purpose of the signs is to:

- Comply with Data Protection Legislation
- Alert individuals of the operation of a CCTV scheme to deter potential criminal activity.

16.3 CCTV signs should be sufficient in number and positioned in such a way to ensure (as far as reasonably possible) that individuals entering an area covered by the scheme are aware that they are entering an area covered by CCTV. The size of signs will vary according to circumstances:

For example – a sign on the entrance door to a site may only need to be A4 size because it is at eye level of those entering the premises.

For example - signs at the entrances of the car parks alerting drivers to the fact that the car park is covered by such equipment will usually need to be large, at least A3 size as they are likely to be viewed from further away, for example by a driver sitting in a car.

The signs should contain the following information:

- Identity of the person or organisation responsible for the scheme.
- The purposes of the scheme.
- Details of whom to contact regarding the scheme.
- To ensure all non-speaking groups are aware of and understand that CCTV is in operation on operational vehicles a CCTV picture signage will also be displayed inside the vehicle saloon where CCTV is activated.

17 Maintenance

17.1 All sites and vehicles should have a service agreement set up with a West Midlands Ambulance Service approved service provider in order to maintain the optimum operation of their system. The service provider should conduct regular service and maintenance inspections of the local system. The service provider should keep the Trusts responsible persons informed of any faults, repairs, or upgrades that are necessary.
18 Fault Reporting

18.1 All faults and malfunctions should be reported without delay to the Estate (Site) or Fleet (Vehicles) departments. They should be reported on the approved pro-forma as directed by the trust and a copy of both the fault log and repair report should be retained by the Trust for a minimum of 12 months. Faulty CCTV does not render the vehicle as VOR.

19 Quality of Images

19.1 It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified. For example, if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

19.2 Cameras should also be regularly maintained in line with the service agreement with an approved service provider. Cameras (particularly external cameras) can become ineffective if they the lenses are not clean or if they are exposed to severe weather conditions. The Trust must have in place a maintenance log in which to record all maintenance work carried out on the system and its cameras, and also undertake a daily/weekly inspection of the quality of the footage being received from the system. The service and work sheets must be obtained and retained for a minimum of 12 months. Vehicle sheets will be maintained by the Fleet department and premises by the Estates department.

20 Disciplinary Procedure

20.1 The information captured by the CCTV recording system will not be used in a disciplinary, sickness and capability issues.

21 Complaints

21.1 Any complaints about this Code of Practice should be addressed to the Trusts Data Controller, and then escalated to the Security Management Director if a satisfactory resolution has not been possible.

22 Breaches of this Policy

22.1 It is recommended that breaches of this Code of Practice by employees should initially be investigated by the Head of Information Governance in order for them to recommend the appropriate action.
Annex A - Correspondence Template for Subject Access Request

Dear Sir/Madam,

Under the terms of the Data Protection Act 1998, 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 West Midlands Ambulance Service NHS Foundation Trust CCTV Policy document, which is available upon request.

The West Midlands 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 be completed and returned on the enclosed form and will 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 or vehicle involved
- A description of the scene where the recording took place i.e. vehicle, Trust building.

All requests will be dealt with in the light of the Data Protection Act 1998 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 Trusts CCTV system are not normally retained for longer than 31 days.

You are reminded that the Trust may not be able to locate your images and payment of any charge does not guarantee that: your image has been recorded, or if it has, that your request will be successful.

Any request will receive an initial reply within 21 days.

For further information please ask for a copy of the West Midlands Ambulance Service NHS Foundation Trust CCTV policy or contact the Trust’s Head of Information Governance or Local Security Management Specialist.
Annex B Subject Access Request Form

Subject Access Request Form

Under Section 7 of the Data Protection Act (1998), access to data that West Midlands Ambulance Service may have of a subject is a subject’s right.

In order to allow West Midlands Ambulance Service to identify and locate the data that you request, please complete all sections of this form and return it to:

Name: 
Address: 
Postcode: 

<table>
<thead>
<tr>
<th>(Section 1) Day of Incident/Visit</th>
<th>Date of Incident/Visit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time of Incident/Visit:</td>
<td>End Time of Incident/Visit:</td>
</tr>
<tr>
<td>Duration of Incident/Visit:</td>
<td></td>
</tr>
</tbody>
</table>

(Section 2) A copy of your ID for West Midlands Ambulance Service employees is required to successfully identify you and confirm the request. Unfortunately West Midlands Ambulance Service can not comply with this request if a copy is not attached.

(Section 3) In order for West Midlands Ambulance Service to consider this request, please provide as much detail as possible as to why you wish to access this data (images/footage). Is there a specific incident that you were involved in that you wish to see?

Details:

(Section 4) Under West Midlands Ambulance Service Code of Practice it is permissible for you to view the data at the Trusts Headquarters rather than be sent the data. If you wish to do this then please tick the box below and send this form back to the site and vehicle. West Midlands Ambulance Service will then endeavour to arrange a mutually convenient time and date for you to attend the Trust Headquarters and view the data.

(Tick box) ☐
(Section 5) I hereby declare that the information that I have given in this subject access request form is true and accurate to the best of my knowledge, and understand that any falsification of information within this request will result in the applicant for access being denied.

I have completed all sections and included both photographic evidence of myself and the correct remittance fee (where applicable).

First Name: ___________________ Surname: ___________________ Signature: ___________________
Date of Request: ___________________

(Section 6) The CCTV System installed inside the sites, vehicles and surrounding land is operated by West Midlands Ambulance Service and is registered with the Information Commissioners Office: Registration Number **********.

The register entry contains personal data collection for 10 purposes, to which Purpose 5 refers to CCTV.

Disclosure of the data captured by the system is restricted to the Police and other legal bodies for use in:

- Crime prevention and crime detection
- The apprehension and prosecution of offenders.

The purpose of the system includes the use of closed-circuit television for the monitoring and collection of sound and/or visual images for the purpose of maintaining the security of premises, for the prevention of crime, and the investigation of crime.

Subject Access to any data should always be addressed to the site and vehicle Data Controller.

All requests for a “Subject Request Form” will be dealt with within fourteen 14 days.

All completed “Subject Request Forms” will be dealt with within forty (40) days, providing all relevant sections have been completed, subject identification can be proven, and the correct remittance is made.

West Midlands Ambulance Service has the right to withhold personal data from an individual where it has been adjudged that the disclosure of the data would be likely to prejudice one or both of the aforementioned purposes.

All CCTV Data is captured by the use of digital/analogue cameras, which can either be fixed or dome mounted (allow for manual operation/movement). All data is stored digitally on a hard drive through the use of a DVR (digital video recorder).
(Section 7) If you are dissatisfied with the outcome of your Subject Access Request and you wish to make a formal complaint, you should put your concerns in writing and address it to:

West Midlands Ambulance Service NHS Foundation Trust  
FAO Head of Information Governance  
Millennium Point  
Waterfront Business Park  
Brierley Hill  
Dudley  
DY5 1LX

An acknowledgement of receipt of your complaint will be sent to you within 5 working days, with a full response, so far as is practical to fully investigate the concern, within fourteen working days.

If you are still dissatisfied with any decision made by West Midlands Ambulance Service NHS Foundation Trust you may then wish to consider taking your complaint to the office of the Information Commissioner:

Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF  
Tel: 01625 545 700

(Section 8) Office Use Only

Date request received:  

Received by:  

Action Taken:  □ Passed to Trust Head of Information and Governance or LSMS.

Date:   

□ Letter sent to subject requesting further information.

Date:   

□ Letter sent to subject refusing access to data.

Date:   

□ Data requested sent to subject.
# Annex C Footage Review Access Log

## West Midlands Ambulance Service

### Footage Review Access Log

The review of CCTV footage or images is restricted to authorised employees and approved external agencies (third parties) only.

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Authorised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Name of Reviewer**

<table>
<thead>
<tr>
<th>Dept./Company</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Details:** (Camera no(s) reviewed, reason for viewing, action taken with footage, etc…)

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Authorised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Name of Reviewer**

<table>
<thead>
<tr>
<th>Dept./Company</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Details:** (Camera no(s) reviewed, reason for viewing, action taken with footage, etc…)

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Authorised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Name of Reviewer**

<table>
<thead>
<tr>
<th>Dept./Company</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Details:** (Camera no(s) reviewed, reason for viewing, action taken with footage, etc…)

<table>
<thead>
<tr>
<th>Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Authorised by</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Name of Reviewer**

<table>
<thead>
<tr>
<th>Dept./Company</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Details:** (Camera no(s) reviewed, reason for viewing, action taken with footage, etc…)

---

Page 20 of 27
Annex D Footage Retention Log

**Footage Retention Log**

Please use this log if it is deemed necessary and appropriate to retain data (images/footage) longer than outlined in the West Midlands Ambulance Service CCTV Code of Practice.

Justifiable reasons for the extended retention may be in order to support any criminal proceedings, or to support in the investigation of any criminal activity. You may also be requested by the Police to extend the retention period of data.

<table>
<thead>
<tr>
<th>Incident Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Camera No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Authorised by:**

**Serial/Security No:**

**Details:** (Reason for extended retention, camera location, description of footage, etc.)

<table>
<thead>
<tr>
<th>Incident Date</th>
<th>Start Time</th>
<th>End Time</th>
<th>Camera No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Authorised by:**

**Serial/Security No:**

**Details:** (Reason for extended retention, camera location, description of footage, etc.)
Annex E Photographic/Image Printing Log

Photographic/Image Printing Log

Please ensure that all photos/images that are printed off are both individually numbered and logged on this form. All photos/images must be shredded when being destroyed to ensure that identification of any person/subject is not possible.

<table>
<thead>
<tr>
<th>Photo No</th>
<th>Date</th>
<th>Incident no (Ulysses)</th>
<th>Type of Incident</th>
<th>Photo Destroyed Date</th>
<th>Destroyed by (Sig.)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex F Genisys Display Panel
Annex G Incident Download Log

Incident Download Log

If there is an incident requiring downloading/copying to be produced this form must be filled out.

Please use BLOCK CAPITALS and fill in BLACK INK

<table>
<thead>
<tr>
<th>1 Incident Details</th>
<th>5 Issued To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Organisations Name and Address including postcode</td>
</tr>
<tr>
<td>Time</td>
<td>Daytime phone number</td>
</tr>
<tr>
<td>Camera Recording Incident</td>
<td>Fax number</td>
</tr>
<tr>
<td>Description of Incident</td>
<td>Email address</td>
</tr>
<tr>
<td>Incident noted by</td>
<td>Mr., Mrs., Miss, MS</td>
</tr>
<tr>
<td>Daytime phone number</td>
<td>Other title (PC)</td>
</tr>
<tr>
<td>Surname</td>
<td>Male, Female</td>
</tr>
<tr>
<td>Forename(s)</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>Organisation Name and Address including postcode</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 Crime Number</th>
<th>6 Archived copy details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Date of download</td>
</tr>
<tr>
<td>Internal Incident Number</td>
<td>Time of download</td>
</tr>
<tr>
<td>Date</td>
<td>Created by</td>
</tr>
<tr>
<td>Police Crime Number/Log Number</td>
<td>Surname</td>
</tr>
<tr>
<td>Date of download</td>
<td>Forename(s)</td>
</tr>
<tr>
<td>Created by</td>
<td>Signature</td>
</tr>
<tr>
<td>Surname</td>
<td></td>
</tr>
<tr>
<td>Forename(s)</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

| 3 Issued Copy Details                      | 7 Destruction                                   |
| Date of download                           | Following completion of investigation the “Archived” copy must be destroyed. |
| Time of download                           | Date of Destruction                             |
| Created by                                 | Name                                            |
| Surname                                    | Signature                                       |
| Forename(s)                                | Witnessed by                                    |
| Signature                                  | Name                                            |

| 4 Disc Serial Number                       | Date of Destruction                             |
| Free text box:                             | Name                                            |
|                                           | Signature                                       |
|                                           | Witnessed by                                    |


Annex H Maintenance Procedure Manual/Footage Retrieval

1 Introduction

1.1 WMAS Emergency Vehicles are fitted with CCTV, there are two different systems in operation dependent on type and age of vehicle. In line with the Vehicle CCTV Policy there will be a requirement for the retrieval of CCTV data from the vehicle system. This is completed by the removal of the memory device (SD Card or Hard Drive) from the CCTV recorder box – workshop staff will have no ability to view footage on the storage media.

1.2 The system also requires checking as part of routine vehicle maintenance inputs. To ensure cameras are operable and orientated correctly and free from obstruction. Defects with the system on each vehicle must be rectified as a matter of priority.

1.3 The reasons for fitting CCTV to our vehicle fleet are;

1.3.1 To contribute to the protection of WMAS staff and its assets.

1.3.2 It is our aim to protect staff safety and welfare and to reduce the overall level of crime (theft, fraudulent claims, property/vehicle damage, and violence) which effects West Midlands Ambulance Service and its stakeholders and also improve employee and public perceptions of their safety and security within West Midlands Ambulance Service.

2 Responsibility

2.1 The General Manager Fleet Services is responsible for oversight of this procedure.

2.2 It is the responsibility of the following personnel to ensure safe and secure retrieval of CCTV data from vehicles and delivery of the storage media to either the Central Fleet Office or Trust Headquarters FAO the LSMS (Local Security Management Specialist);

- Head of Engineering
- Workshop Supervisors

2.3 It is the responsibility of all Fleet Workshop staff tasked with retrieval of CCTV storage media that they do so in accordance with this procedure and the Trusts Vehicle Closed Circuit Television Policy.

2.4 In the case of a vehicle accident, it is the responsibility of crews to
complete accident report forms in a timely manner to assist the fleet team identify a requirement for retrieval of CCTV data.

2.5 In accordance with the Vehicle CCTV Policy it is important that EOC make the General Manager Fleet Services & LSMS (Local Security Management Specialist) aware of all occasions where the crew have activated the CCTV recording function (in the rear saloon).

2.6 It is the responsibility of the following personnel to ensure the system is checked for correct operation during workshop inputs.

- Head of Engineering
- Workshop Supervisors

3 Procedure

3.1 Footage Retrieval

3.1.1 Additional (replacement) CCTV data storage media devices are held by the Fleet Department. This facilitates the removed media device being replaced immediately.

3.1.2 On notification of a requirement to retrieve CCTV data, the workshop supervisor will liaise with EOC and operational management to ensure the vehicle is available and allocate the task – it should be noted that timely retrieval of the memory device is important, and takes place within 12hrs.

3.1.3 Staff tasked with retrieval of the CCTV data storage device should attach a label on the removed device annotated with:

a. Name of person carrying out task
b. Time and Date memory device removed
c. Fleet Number and Registration Number of vehicle
d. Type of vehicle (RRV or DMA)

3.1.4 The CCTV data storage device is to be placed and sealed in an envelope, marked ‘Private & Confidential’ and delivered to the Central Fleet Office FAO GM Fleet Services or Headquarters FAO the LSMS (Local Security Management Specialist) ASAP.
3.2 System Maintenance

3.2.1 During maintenance inputs a visual inspection of the CCTV cameras will be undertaken, anything obscuring the clear view of the camera should be removed and where necessary reported to the workshop supervisor.

3.2.2 At least twice a year the system will be checked by workshop staff during a scheduled maintenance input, the following checks will be carried out:

- Remote screen connected to system
- All cameras are orientated correctly
- All inputs are displaying correctly – eg Sirens, Blue Lights, Headlamp Flash, Brakes and Indicators

3.2.3 The system maintenance is to be recorded on a workshop job card In accordance with normal procedures.

4 References

Trust Policy Document - Trusts Vehicle Closed Circuit Television Incident Reporting Policy/Procedure
Vehicle Accident Reporting Procedure