Closed Circuit Television Policy and Code of Practice

Document Profile Box

<table>
<thead>
<tr>
<th>Document Reference:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td>0001</td>
</tr>
<tr>
<td>Ratified by:</td>
<td></td>
</tr>
<tr>
<td>Date ratified:</td>
<td>March 2010</td>
</tr>
<tr>
<td>Name of originator/author:</td>
<td>Alan Gallagher</td>
</tr>
<tr>
<td>Name of responsible committee/individual</td>
<td>Assurance Committee</td>
</tr>
<tr>
<td>Date issued:</td>
<td>March 2010</td>
</tr>
<tr>
<td>Review date:</td>
<td>February 2011</td>
</tr>
<tr>
<td>Target audience:</td>
<td>As prescribed in Policy</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Introduction</td>
<td>4</td>
</tr>
<tr>
<td>2 Aim</td>
<td>4</td>
</tr>
<tr>
<td>3 Objectives</td>
<td>5</td>
</tr>
<tr>
<td>4 Statement of Intent</td>
<td>6</td>
</tr>
<tr>
<td>5 Responsibilities</td>
<td>6</td>
</tr>
<tr>
<td>6 Training</td>
<td></td>
</tr>
<tr>
<td>7 Operation of the system</td>
<td>7</td>
</tr>
<tr>
<td>8 Road Traffic Collision Activation</td>
<td>7</td>
</tr>
<tr>
<td>9 Saloon Activation</td>
<td>8</td>
</tr>
<tr>
<td>10 Trust Premises</td>
<td>9</td>
</tr>
<tr>
<td>11 Control Room</td>
<td>11</td>
</tr>
<tr>
<td>12 Monitoring procedures</td>
<td>12</td>
</tr>
<tr>
<td>13 Covert surveillance</td>
<td>12</td>
</tr>
<tr>
<td>14 Digital recording</td>
<td>12</td>
</tr>
<tr>
<td>15 Retaining information</td>
<td>13</td>
</tr>
<tr>
<td>16 Access to the images</td>
<td>13</td>
</tr>
<tr>
<td>17 Police Access to Hard Drives</td>
<td>14</td>
</tr>
<tr>
<td>18 Third Party Access to Hard Drives</td>
<td>14</td>
</tr>
<tr>
<td>19 Subject Access requests</td>
<td>14</td>
</tr>
<tr>
<td>20 Signage</td>
<td>15</td>
</tr>
<tr>
<td>21 Maintenance</td>
<td>16</td>
</tr>
<tr>
<td>22 Fault Reporting</td>
<td>16</td>
</tr>
<tr>
<td>23 Quality of Images</td>
<td>17</td>
</tr>
<tr>
<td>24 Compliance with the Code of Practice</td>
<td>17</td>
</tr>
<tr>
<td>25 Disciplinary Procedure</td>
<td>17</td>
</tr>
<tr>
<td>26 Clinical Negligence</td>
<td>17</td>
</tr>
<tr>
<td>27 Complaints</td>
<td>17</td>
</tr>
<tr>
<td>28 Breaches of this Policy</td>
<td>17</td>
</tr>
<tr>
<td>29 Site and Vehicle Specifics</td>
<td>18</td>
</tr>
<tr>
<td>30 System Details</td>
<td>19</td>
</tr>
<tr>
<td>31 Offences</td>
<td>20</td>
</tr>
<tr>
<td>32 Glossary of Terms</td>
<td>21</td>
</tr>
<tr>
<td>33 Equality and Diversity statement</td>
<td></td>
</tr>
<tr>
<td>34 Dissemination and Implementation</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
</tr>
<tr>
<td>35</td>
<td>Consultation, Approval and Ratification Process</td>
</tr>
<tr>
<td>36</td>
<td>Monitoring Compliance</td>
</tr>
<tr>
<td>37</td>
<td>Review and Revision Arrangements including Version Control</td>
</tr>
</tbody>
</table>

**Appendices**

- Appendix A  Control Room Visitor Access Log Template
- Appendix B  Subject Access Correspondence Template
- Appendix C  Subject Access Request Form Template
- Appendix D  Data Protection Training Log Template
- Appendix E  Footage Review Access Log Template
- Appendix F  Footage Retention Log Template
- Appendix G  Photographic/Image Printing Log Template
- Appendix H  Covert Surveillance Request Form Template
- Appendix I  Investigation Observation Log Template
- Appendix J  Certificate of Training
- Appendix K  Approved Persons to Access/Maintain CCTV System
- Appendix L  Access to View or Copy Images – Police
- Appendix M  Version Control Sheet
- Appendix N  Equality Impact Assessment Screening Tool
1 Introduction

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

The systems in each site/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.

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.

The CCTV system is owned by North East 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: North East Ambulance Service NHS Trust, Bernicia House, The Waterfront, Goldcrest Way, Newburn Riverside, Newcastle, NE15 8NY

2 Aim

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

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

2.3 It is also our aim to reduce the overall level of crime (theft, fraud, property damage, violence) which effects North East Ambulance Service and it’s stakeholders and also improve employee and public perceptions of their safety and security within North East Ambulance Service.

2.4 In pursuit of this aim, North East Ambulance Service will:

- Operate a CCTV system for monitoring activity within sites and vehicles and other high risk areas in order to provide enhanced security and evidential quality recordings of criminal activity and breaches of Health & Safety.
- Ensure that all employees operating the CCTV system are appropriately trained, accredited, and vetted.
- Ensure that the system is operated in accordance with the Data Protection Act (1998) and its associated guidance and ACOP (approved code of practice).
- Ensure that proper management and control procedures are in place to protect the integrity and security of all recordings made using the CCTV system.
- Extend the CCTV system where a local demand is assessed and deemed necessary and where local capital/revenue funding allows.
• Pursue (locally) opportunities to integrate the CCTV system into a wider security provision for crime reduction initiatives and other related schemes.

2.5 This policy details the circumstances when the CCTV recording system may be used by North East Ambulance Service NHS 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 property or 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 serious road traffic collision involving a North East 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 (see sections 7 and 8 below).

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.

3 Objectives of the CCTV Scheme

3.1 This policy applies to all ambulance 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.

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

• Protecting the Trust sites, vehicles, buildings and its assets
• To increase personal safety and reduce the fear of crime
• To assist in identifying, apprehending and prosecuting offenders
• To protect members of the public and private property
• To assist in managing the Trust sites and vehicles
• To support the Police in a bid to deter and detect crime
• Preventing and investigating crime or assisting with road traffic collision investigations.
  i.e. protecting Trust property from theft and employees from acts of violence and aggression by patients or any other member of the public, or establishing an accurate account of events surrounding a serious road traffic collision.

3.3 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.

3.4 Access to recorded material shall only take place as defined in this policy.
3.5 Recorded material shall not be sold or used for commercial purposes or the provision of entertainment.

3.6 The showing of recorded material to the public shall only be allowed 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 Cameras will be used to monitor activities within the sites and vehicles to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well being of the stakeholders, sites and vehicles.

4.4 Materials, footage, or knowledge 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 North East Ambulance Service Data Controller based at Bernicia House Headquarters and of the Police. Footage will never be released to the media for purposes of entertainment.

4.5 The planning, design, and approval of the site and vehicle CCTV system has endeavored to ensure that the system will 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 areas of coverage.

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

5 Responsibilities

5.1 The Director of Finance and Performance, as the Security Management Director (SMD), has overall legal responsibility for the Trust's CCTV system(s).

5.2 The Trusts Head of Risk and Claims and LSMS (Local Security Management Specialist) are 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 Trusts Head of Risk and Claims and LSMS (Local Security Management Specialist) are responsible for the downloading, storage and use of any images gathered. It is also the post holder's responsibility to liaise with the Police or other interested parties if required following such an incident.

5.4 The Fleet Manager shall be responsible for the installation and maintenance of the CCTV recording system within vehicles in consultation with the Trust's Head of Risk and Claims and LSMS.
5.5 The Head of Estates shall be responsible for the installation and maintenance of CCTV systems within buildings and premises in consultation with the Trust’s Head of Risk and Claims and LSMS. It is the responsibility of the Trust’s Head of Risk and Claims and LSMS for 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.

5.6 The Trust’s Head of Risk and Claims and LSMS shall be responsible for maintaining secure access to all recordings which may be captured by the CCTV recording system on the system’s recording media. The post holder’s are also responsible for ensuring that the images captured and recorded by the systems are of an appropriate quality; and, that logs of inspection, maintenance and repair work in respect of the CCTV systems are properly maintained and audited.

5.7 The designated third party contractors shall be responsible for the day to day maintenance and servicing of the CCTV recording system on all vehicles and sites.

5.8 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.

6 Training

6.1 Information, instruction and training in the requirements of the law on Data Protection will be given to staff who are required to manage and work the CCTV systems.

6.2 Staff will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation.

6.3 Training by CCTV system installers will also be provided as appropriate.

6.4 General information regarding the systems and the requirements of the law will be communicated to all Trust staff via this policy and other reference documents/media’s.

7 Operation of the System

7.1 The systems will be administered and managed by the Head of Risk and Claims and the Local security Management Specialist, in accordance with the principles and objectives expressed in this policy.

7.2 The overall responsibility to ensure that the Trust adheres to this Code of Practice lies with the Head of Risk and Claims based at Bernicia House Headquarters.

7.3 The day-to-day management will be the responsibility of the Trust’s Head of Risk and Claims, Trusts Local Security Management Specialist and the Fleet Manager.

7.4 Operating the system should be restricted to only those who have been suitably trained, accredited, and vetted. Accreditation and vetting should now be done through the SIA (Security Industry Authority) which is a legal requirement.

7.4 The 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 Risk and Claims Department based at Bernicia House Headquarters.

8 Road Traffic Collision Activation

8.1 This policy covers the operational use of the vehicles saloon, front, near-side and rear facing CCTV recording facility.
8.2 The CCTV recording system is operated from the vehicle ignition system and automatically powers down 15 minutes after the vehicle ignition is switched off. The CCTV system automatically powers up on activation of the vehicle’s ignition.

8.3 Whilst powered up, the CCTV system is programmed to record whenever there is movement within the cameras field of view. Whilst movement occurs the camera will continue to record, whenever movement ceases the camera will continue to record for a predetermined length of time, that length of time will vary according to the application of each particular camera, however it will not exceed 4 minutes in any case. All recordings will be written to the CF card in the DVR (Digital Video Recorder), the size of the CF (Compact flash) card is specified to allow 14 days of footage to be retained, however this may vary and in some cases retention may be less or more depending upon frequency of use of the vehicle.

Whilst footage is retained for the period of 14 days, the Trust is legally obliged to only view footage in relation to an actual event or potential event. The persons authorised to review footage must not view any unrelated footage or use the historical footage without justification and evidence to support this.

8.4 The unit will be activated by a serious road traffic collision outside of the vehicles Incident Data Recorders (IDR) pre-set parameters. The IDR and CCTV units will record in tandem thus capturing vital evidence surrounding the lead up to the incident and ensuring that all relevant evidence is preserved for investigation, insurance claims purposes and potentially production in court if required.

8.5 The digital recorder is installed in a locked cabinet within the vehicle; the cabinet is fitted with a specific security lock to which only authorised personnel have access. These personnel will be identified prior to use of the system. 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 CF cards is logged into the memory of the DVR unit and is tagged with a time and date.

8.6 Any security keys issued to authorised personnel must be kept in safe and secure locations.

8.7 As part of the ensuing investigation process following a serious road traffic collision, the following information will be recorded and included within the Investigation Report document

a. The date and time of removal.
b. The name of the person removing the CF card.
c. The name(s) of the person(s) viewing the images. This should include third parties.
d. The reason for viewing.
e. The date and time the CF was returned to the system or secure place, and if they have been retained for evidential purposes.

9 Saloon Activation

9.1 This policy covers the operational use of the new vehicle CCTV within the saloon of the vehicle.

9.2 As 8.2 above
9.3 Whilst powered up, the CCTV system is programmed to record whenever there is movement within the camera's field of view. Whilst movement occurs the camera will continue to record, whenever movement ceases the camera will continue record for a predetermined length of time, that length of time will vary according to the application of each particular camera, however it will not exceed 4 minutes in any case. All recordings will be written to the CF card in the DVR (Digital Video Recorder), the size of the CF (Compact flash) card is specified to allow 14 days of footage to be retained, however this may vary and in some cases retention may be less or more depending upon frequency of use of the vehicle. During movement activation audio recording is operational; this is for use when investigating cases of physical and verbal abuse.

9.4 Antibacterial panic strips are located in the saloon of the vehicle and when pressed will bookmark recording to help identify quickly footage related to incidents that have required use of the panic strip.

9.5 As 8.5 above

9.6 As 8.6 above

9.7 All CF cards which are not secured within a CCTV system will be kept secure under locked conditions by the Trust's Head of Risk and Claims and Local Security Management Specialist. Any hard disk or duplicate hard disk which is supplied to an approved third party must be kept in a secure location.

9.8 If a saloon activation of a potential incident has taken place the person who activated the CCTV recording system must contact the Trust's Head of Risk and Claims and Local Security Management Specialist and record the event on the Incident Reporting form NEAS07. If the person who activated the CCTV recording system is not able to contact the Trust's Head of Risk and Claims or Local Security Management Specialist any other member of staff, who is aware of its activation, must contact the Trust's Head of Risk and Claims or Local Security Management Specialist and record the event on an NEAS07. The Trust's Head of Risk and Claims or Local Security Management Specialist will then take steps to remove the CF card to a secure place to act as evidence or as necessary to erase the recording within seven days.

9.9 On removal or production of images for use in legal proceedings the Trust's Head of Risk and Claims or Local Security Management Specialist will ensure the following is documented and recorded on the relevant documents:

   a. The date on which the images were removed from the system for use in legal proceedings.
   b. The reason why they were removed from the system.
   c. Any crime incident number to which the images may be relevant.
   d. The location of the images and any other relevant information.
   e. The signature of the collecting Police Officer

9.10 On removal of the recording media for viewing purposes the Trust's Head of Risk and Claims or Local Security Management Specialist will ensure the following is documented and recorded on the appropriate documents:

   a. The date and time of removal.
   b. The name of the person removing the hard drive.
   c. The name(s) of the person(s) viewing the images. If this should include third parties, this should include the organisation of that third party.
   d. The reason for viewing.
   e. The outcome, if any, of the viewing.
f. The date and time the hard drive is returned to the system or secure place, if they have been retained for evidence purposes.

9.11 Removal of the CF card for maintenance purposes should be documented as follows by the Trusts appointed provider and recorded details passed to the Trusts Head of Risk and Claims or Local Security Management Specialist for documenting.

   a. The date and time of maintenance.
   b. The name of the person performing the maintenance.
   c. The reason for the maintenance.
   d. Type of maintenance being carried out.

10 Trust Premises

10.1 North East Ambulance Service NHS Trust currently uses a 24 hour close circuit television system which are in operation in some of its premises.

10.2 Images will not be retained for any longer than necessary, up to a maximum of 31 days unless they are required in respect of the investigation of an alleged crime.

10.3 If a potential security breach has taken place it will be the responsibility of the site Manager or other designated members of staff to assess whether any CCTV images may have captured the details of the incident.

10.4 If there is any possibility that such images may have been captured the site Manager must contact the Trusts Head of Risk and Claims or Local Security Management Specialist and make them aware that a relevant recording may have taken place. The same collecting and sorting process will apply as described in section four.

10.5 CCTV cameras will be sited in such a way that they can only monitor areas intended to be monitored by the equipment. Staff involved in the operation of the CCTV equipment will be made aware they are only able to use the equipment for the purpose of maintaining the security of premises, preventing and investigating crime. CCTV monitors will be sited so that they can only be accessed and viewed by authorised personnel.

11 CCTV Room

11.1 The Risk/Security responsible must check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.

11.2 Restricted Access to the CCTV Control Room/system should be in place and should be limited to members of the list of authorised personnel and visitors/contractors who are required to undergo essential maintenance or repairs on the system.

11.3 Visitors and other contractors wishing to enter the CCTV Room will be subject to particular arrangements, which are as follows:

   • A log book (visitor book) should be in place in all CCTV rooms to record the attendance of all visitors.

   • CCTV Room Operators must satisfy themselves over the identity of any other visitors to the CCTV Room and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors must be logged in the CCTV Room log book.

   • Casual visits will not be permitted and employees should not allow access to the control room, CCTV monitors, or CCTV footage to their family, friends or un-authorised persons.
• Visitors and contractors requiring access to the CCTV room must first obtain permission from the Trusts Head of Risk and Claims or Local Security Management Specialist, or their deputy in order to gain access.

• There must always be at least one authorised employee representative present within the CCTV Room at all times. This is to ensure that the integrity of the system is not breached, and that all life critical systems are monitored / managed.

• If it is at all not possible to man the CCTV room then it must be ensured that the room can be locked / secured, and access restricted to those with appropriate access rights.

12 Monitoring Procedures

12.1 Camera surveillance must be maintained at all times. Monitors will be installed in a way that does not allow easy access to the general public or non authorised employees, to which pictures will be continuously recorded.

12.2 The monitoring of images may only be undertaken by authorised employees/third parties who have been authorised by the Trusts nominated Data Controller.

12.3 A copy of the CCTV Code of Practice which sets out the measures which must be adopted to comply with the Data Protection Act 1998 is available from the Information Commissioners (ICO) @: http://www.ico.gov.uk/Home/for_organisations/topic_specific_guides/cctv.aspx

13 Covert Surveillance

13.1 Regulation of Investigatory Powers Act (2000) legislation exists to ensure that the relevant investigatory powers are used in accordance with human rights. This legislation covers the purposes for which covert surveillance may be used, which authorities can use the powers, who should authorise each use of the powers, the use that can be made of the material gained and a means of redress for the individual. Further information can be obtained from The Office of Public Sector Information website www.opsi.gov.uk

13.2 There are also strict guidelines issued by the Information Commissioner with regard to covert filming. Covert filming should only be undertaken with approval from both the Trusts Security Management Director and the Head of Risk and Claims or Local Security Management Specialist (or in their absence their deputies).

13.3 The Trust will consider if it is permissible to inform the relevant Trade Union(s) of any potential installation of covert monitoring equipment. This will be heavily reliant upon advice and guidance from Police authorities and other relevant parties. Where it is appropriate and permissible a nominated senior union official should be advised that covert surveillance is occurring at the earliest possible opportunity.

13.4 Covert monitoring means monitoring carried out in a manner calculated to ensure those subject to it are unaware that it is taking place, and that notifying employees about the monitoring would prejudice the prevention or detection of any criminal activity or equivalent malpractice.

13.5 There should be a clear and specific criminal activity identified and an assessment undertaken as the need to use covert surveillance to obtain evidence of that criminal activity. The information obtained must only be for the prevention or detection of criminal activity or equivalent malpractice, or the apprehension and prosecution of offenders. It should not be retained and used for any other purpose.
13.6 Also, if the equipment being used has a sound recording facility, this should not be used to record conversations between members of the public.

13.7 All applications for the installation of covert equipment should be made on the approved North East Ambulance Service Covert Surveillance form (see appendix.), and no installation should take place until this form has been completed and approved.

NOTE: Covert monitoring should not normally be considered. It will be rare for covert monitoring of employees to be justified. It should therefore only be used in exceptional circumstances.

13.8 The following must be in place and recorded before covert monitoring can take place:

• There must be a set time frame in place (start date and end date).
• Surveillance must cease once this agreed time frame has elapsed.
• Surveillance can only be extended by the Head of Risk and Claims or the Security Management Director.
• Access to the images/footage should be restricted.
• Number of employees involved in the investigation should be limited.

14 Digital Recording

14.1 All systems within North East Ambulance Service sites and vehicles should be recording images digitally onto a hard drive with the use of a DVR or in the case of vehicle systems onto a compact flash card.

14.2 Digital systems allow for ease of storage, playback, and editing. Editing of footage is prohibited other than to capture footage of a specific time frame/period and therefore editing out unnecessary footage before or after the required time frame/period. Employees should at no time attempt to manipulate or edit footage/images in any way that will prevent it from being viewed in its original captured form. This includes changing colours, the date/time stamp, integrating two images into one, and so on.

14.3 The Trust’s current CCTV systems do not form a part of the current Information Technology (IT) infrastructure and do therefore not form a part of the IT strategy.

14.4 For systems that have not yet upgraded to digital recording then the following must be in place:

• All tapes must be numbered and identifiable by day/date.
• All tapes must be kept secured in a lockable cabinet.
• Access to the tapes must be restricted to authorised employees.
• Copying, editing, and loaning of any tapes must first be authorised by the Trusts Data Controller.
• Images need to be of a good quality; therefore all tapes need to be changed after 6 uses.
• Footage must not be recorded over old/previous footage and as such the use of a tape cleaning/degaussing machine must be used on each tape before each use.

15 Retaining Information

15.1 It is important that images are not retained for longer than is considered necessary for the purpose for which they were processed. While images are retained, it is essential that their integrity is maintained, for both evidential purposes and to protect the rights of those individuals captured in the images.
15.2 Images should not be retained for longer than 31 days unless they are required for evidential purposes in legal proceedings or are needed in support of any on-going investigations. The only exception to this rule is cameras sighted on till points, which may be retained for 90 days. This is in order to support financial institutions and banking systems with matters of fraud and deception.

15.3 The retention periods detailed within this document are based on guidelines and are the approved periods identified by the North East Ambulance Service.

15.4 Images that are required to be retained for longer than the approved times stated above should be retained securely (preferably in a sealed bag and stored within a secure area) and clearly marked as to why it is being retained. The footage should also be logged on the approved North East Ambulance Service Footage Retention Log form (see appendix.); with regular inspections being carried out by the Trusts Data Controller to ensure that the footage/material is still relevant and has not been tampered with.

16 Access to the Images

16.1 It is important that access to, and the disclosure of, images to third parties is strictly controlled and documented. This is to ensure that the rights of the individual are maintained and that the chain of evidence remains intact should the images be required for evidential purposes.

16.2 Camera recording equipment is positioned in a locked cabinet on board the vehicle that prevents unauthorised access and camera recording can only be viewed if the correct software and appropriate passwords/clearance is available (authorized persons only).

16.3 Access to camera recordings and associated equipment is limited to a small number of authorised Trust representatives only.

16.4 No operational staff and managers will have access to camera recording equipment at any time unless accompanied by an authorised person and acting in compliance with this policy.

16.5 Recordings will only be accessed by and provided to authorised person/s in the event of a formal request to do so or following a reported incident.

16.6 Employees should not disclose any images or material to anyone outside of North East Ambulance Service or to any other un-authorised employee without the expressed permission of the Trusts Data Controller. This includes e-mailing images/footage, downloading images/footage, or printing images/footage.

16.7 If access to images by third parties is required in order to support legal proceedings or to defend a claim (i.e. police, solicitors, insurance, etc.) then access to this footage must be strictly regulated and documented. All footage/material released for this purpose must be documented on the approved North East Ambulance Service Access to Images Log form (see appendix.) and approved by the Trusts Data Controller.

17 Police Access to Hard Drives and or other Recording Medias

17.1 Police may apply for access to hard drives and or other recording media, by agreement, where they reasonably believe that access to specific media is necessary for the investigation and detection of a particular offence or offences, or for the prevention of crime.

17.2 Police may obtain access to hard drives and or other recording media under the provision of the Police and Criminal Evidence Act 1984 (PACE). Police requesting data from the systems should be made in writing to the Trust's Information Governance Manager or Head
of Risk and Claims and LSMS (Local Security Management Specialist) and should state that the purpose of the request and, as clearly as possible, how failure to disclose would 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.”

17.3 Staff shall be required to provide the police with statements required for evidential purposes.

18 Third Party Access to Hard Drives and or other Recording Media

18.1 Access to hard drives and or other recording media may be obtained in connection with civil disputes by court order or extended to lawyers acting for defendants or victims in connection with criminal proceedings.

18.2 No other access shall be allowed unless approved by the Director of Finance and Performance or the Trust’s Head of Risk and Claims or Local Security Management Specialist who will review requests in line with the purpose and objectives of the scheme and in accordance with the policy.

19 Subject Access Requests

19.1 Under Data Protection legislation, an individual has the right to view any personal information held about them by an organisation. All requests should be made on the North East Ambulance Service approved Subject Access Form (see appendix.). A fee of £10 may be levied against the subject for the administration of this request.

19.2 All Subject Access requests must be directed to the Trusts Data Controller and they must respond to the request within forty days (40 days) of receipt of the request. However, unless the Trusts Data Controller has received a request in writing, received the prescribed fee, and received supporting evidence (preferably photographic) in order to identify the subject, and 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.

19.3 Unfortunately the request for information that North East Ambulance Service holds on a Data Subject is sometimes requested for no reason other than to cause disruption to the Trusts operation. Therefore the Trust Data Controller 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. North East Ambulance Service considers this reasonable time lapse to be three months (3 months) or more unless there has been another incident.

19.4 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.

19.5 If the site and vehicle Data Controller is going to refuse the request then they must inform the subject of their decision and to the reasons why within fourteen days (14 days), which
allows the subject a reasonable amount of time to contest the reasons as to why and provide further information/identification, etc. A letter must be sent to the subject advising them of this.

19.6 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. If after viewing the footage the data subject still requires a copy of the footage then a fee of £10 may be levied against them for the administration of this request.

19.7 The Trust retains the right as data controller to make the ultimate decision on disclosure of CCTV images

20 Signage

20.1 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.

20.2 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.

20.3 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.

For example - Where an image of a camera is not used on a sign – the following wording should be used:
"Images are being monitored for the purposes of crime prevention and public safety. This scheme is controlled by North East Ambulance Service NHS Trust. For further information contact 0191 430 2143".

For example – Where an image of a camera is used on a sign – the following wording should be used:
"This scheme is controlled by North East Ambulance Service NHS Trust. For further information contact 0191 430 2143".
In exceptional and limited cases, if it is assessed that the use of signs would not be appropriate (i.e. during covert surveillance), the Trusts Data Controller must ensure that they have:

- Identified specific criminal activity.
- Identified the need to use surveillance to obtain evidence of that criminal activity.
- Assessed whether the use of signs would prejudice success in obtaining such evidence.
- Assessed how long the covert monitoring should take place to ensure that it is not carried out for longer than is necessary.
- Documented all of the above.

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

20.5 Latest CCTV equipped vehicles (post August 2009) will have a small LED underneath the saloon camera dome and appropriate signage advising that when illuminated the system is recording. In addition to this these vehicles will have the facility whereby upon closure of the vehicle saloon doors, an audio message will play and communicate the following message:

“For the safety of our staff and service users, this vehicle is fitted with CCTV and images will be recorded for the prevention and detection of crime”

21 Maintenance

21.1 All sites and vehicles should have a service agreement set up with a North East 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.

21.2 The service provider should also provide a “loan of equipment” service, while any faults are being rectified.

22 Fault Reporting

22.1 All faults and malfunctions should be reported without delay to the service provider. They should be reported on the approved pro-forma as instructed by the service provider and a copy of both the fault log and repair report should be retained by the Trust for a minimum of 12 months.

22.2 In addition, the Risk and Claims Management department should also be informed of any faults/malfunctions that would prevent the system from monitoring/recording images.

23 Quality of Images

23.1 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.

23.2 North East Ambulance Service has identified industry standards for quality of images and as such has adopted to follow these standards. Suppliers of CCTV Systems for North East Ambulance Service sites and vehicles should install cameras which capture and record images at approved industry standards.
23.3 If the system in place records features such as the location of the camera, the camera number, the date/time then this must be accurate. The Trusts Data Controller or system responsible should ensure that they have a documented procedure in place to regularly (daily) check the accuracy of this information.

23.4 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.

24 Compliance with the Code of Practice

Performance monitoring, including random operating checks may be carried out by the Trusts Data Controller, and members of the Internal and External Audit Teams.

25 Disciplinary Procedure

The information captured by the CCTV recording system may only be used for the purposes as described in 3.2 and may not be used against any staff member in any disciplinary hearing unless in connection with the use as outlined in 3.2.

26 Clinical Negligence

The information captured by the CCTV recording system may only be used for the purposes as described in 3.2 and may not be used against any staff member in any allegation of clinical negligence unless in connection with the use as outlined in 3.2.

27 Complaints

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.

28 Breaches of this Policy

It is recommended that breaches of this Code of Practice by employees should initially be investigated by the Trusts Data Controller in order for them to recommend the appropriate disciplinary action.

29 Site and Vehicle Specifics

29.1 Reversing Camera

All post August 2009 coach built ambulance vehicles come with a reversing camera that is to be used as a reversing aide for staff. This camera also records via motion detection at 2 frames per second (fps) as standard, the reversing camera activates automatically on selection of reverse gear and staff can then see a view behind the vehicle in a screen mounted in the cab in place of a rear view mirror.

29.2 Forward Facing Camera
A camera is fitted behind the rear view mirror, in accordance with forward vision legislation, and will record upon movement at 6 fps. The camera is positioned in such a way that images will be recorded from the area directly in front of the ambulance and beyond. This camera image will incorporate vehicle information such as vehicle speed, operation of indicators, brakes, lights, headlight flash (hlf) sirens and blues.

29.3 Side Camera

A vandal resistant dome camera is installed directly above the side, sliding door and will record upon movement at 2fps. This camera is positioned in such a way that images will be recorded from a view directly adjacent to the ambulance.

29.4 Saloon Camera

A vandal resistant dome camera, mounted in the roof, is located in a position that covers the internal area of the ambulance; the placement is such that if the staff are physically or verbally abused the incident will be recorded onto the compact flash card at 6fps, the vehicle saloon camera and recording system has been fitted and set up in a way that supports compliance with the following legislation and national guidance, as well as the NHS and Trust policies.

- CCTV Code of Practice Revised edition 2008
- Human Rights Act 1998 (Came in to effect in the UK October 2000)
- Data Protection Act 1998
- NHS Integrated Information Governance Framework
- NHS code of confidentiality
- NEAS Records Management Policy
- NEAS IT Security Policy

29.5 To ensure compliance with the above legislation, policies and guidance the CCTV camera and recording system has been set up in the following way:

- A static, vandal resistant camera is built in to the roof of the saloon of the vehicle positioned so that it has a whole view of the saloon area
- A microphone is fitted so sound will be recorded as standard
- On activation of the panic strip fitted in the saloon a visual warning red light will come on and stay on in saloon area and a synthesised voice system will provide a verbal warning “that recording is in progress” every 5 minutes while the recording system is active.
- In the event of an accidental activation and the system alarms are sounding, the audible alarm can be manually switched off by a crew member from a switch panel in cab.
- Recordings are time and date stamped so should be admissible as evidence in a court of law (if required)
- Recordings will automatically overwrite on the vehicle and site systems unless accessed/removed/stored within a specified time period.
- All recording material will be stored in line with national guidance and Trust policies
## System Details

<table>
<thead>
<tr>
<th>Trust Data Controller</th>
<th>North East Ambulance Service NHS Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Bernicia House, The Waterfront, Goldcrest Way, Newburn Riverside, Newcastle, NE15 8NY</td>
</tr>
<tr>
<td>Administration Responsible</td>
<td></td>
</tr>
<tr>
<td>Contact Number</td>
<td>0191 430 2000</td>
</tr>
<tr>
<td>ICO Registration Number</td>
<td></td>
</tr>
</tbody>
</table>

### Vehicles

| No of static cameras | 4 cameras fitted into each coach built ambulance post August 2009 |
| No of dome cameras   |                                                            |
| Type of system       | Digital                                                    |

| System Supplier       | Vision Unique Equipment Ltd                                |
| Address               | Unit 7, Ashburton Park, Wheel Forge Way, Trafford Park, M17 1TD |
| Contact No            | 0161 877 2257                                              |

| Service Agreement Supplier |                                        |
| Address                     |                                        |
| Contact No                  |                                        |
| Service Agreement No        |                                        |

<p>| Premises                   | Bernicia House, The Waterfront, Goldcrest Way, Newburn Riverside, Newcastle, NE15 8NY |
| No of static cameras       |                                                            |
| No of dome cameras         |                                                            |
| Type of system             |                                                            |</p>
<table>
<thead>
<tr>
<th>System Supplier</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement Supplier</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Premises</th>
<th>Russell House, Unit 6 Monkton Business Park, Mill Lane, Hebburn NE31 2JZ</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of static cameras</td>
<td></td>
</tr>
<tr>
<td>No of dome cameras</td>
<td></td>
</tr>
<tr>
<td>Type of system (digital/analogue):</td>
<td></td>
</tr>
<tr>
<td>System Supplier</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement Supplier</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement No</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Premises</th>
<th>Pallion (Ambulance Station, Workshops and Equipment/Stores), Pallion West Industrial Estate, Pallion, Sunderland SR4 6SJ</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of static cameras</td>
<td></td>
</tr>
<tr>
<td>No of dome cameras</td>
<td></td>
</tr>
<tr>
<td>Type of system (digital/analogue):</td>
<td></td>
</tr>
<tr>
<td>System Supplier</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement Supplier</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Contact No</td>
<td></td>
</tr>
<tr>
<td>Service Agreement No</td>
<td></td>
</tr>
</tbody>
</table>
31 Offences Under the Act

31.1 North East Ambulance Service’s CCTV Code of Practice has been designed and implemented in order to ensure that as an organisation we conform to the Data Protection Act (1984), and also follow best practices/recommendations as laid down in the Information Commissioners Code of Practice.

31.2 The CCTV Code of Practice has the dual purpose of assisting operators of CCTV Systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

31.3 The Data Protection Act has laid down some principles that must be followed in order to comply with the Data Protection Act and also its code of Practice, they are:

- The data must be fairly and lawfully processed.
- Personal data must be adequate, relevant and not excessive in relation to the purposes for which it is processed.
- Personal data must be accurate and, where necessary, kept up to date.
- Personal data must not be kept longer than necessary for the purposes for which it is processed.
- Personal data must be processed in accordance with the rights of data subjects under the Act.
- Personal data must be subject to appropriate technical and organizational measures to protect against unauthorized or unlawful processing and accidental loss, destruction or damage.
- Personal data must not be transferred to a country or territory outside of the European Union unless that country or territory ensures an adequate level of Data Protection.

31.4 Unless North East Ambulance Service follow these principles then it may be in breach of the Data Protection Act, and there are a number of offences that can be committed, which include:

- Processing without notification.
- Failing to notify the Commissioner of changes in your circumstances.
- Failing to comply with written requests.
- Failing to comply with enforcement notices.
- Knowingly or recklessly making false statement in compliance with an information notice.
• International obstruction of or failure to give reasonable assistance in an execution of a warrant.

It is also an offence for an employee without the consent of the Data Controller, knowingly or recklessly to:

• Obtain or disclose personal data or the information contained in personal data.
• Unlawful selling of personal data.
• Unlawful disclosure of information by commissioner/staff/agent.

31.5 All of these offences may be tried in either the Magistrates Court or the Crown Court. Upon conviction in the Magistrates Court, an offender is liable to a maximum fine of £5000. Whilst in the Crown Court an unlimited fine may be imposed.

31.6 The Act also provides for separate liability for the offences in the Act for Directors or other senior management of the company which has committed the offence.

32 Glossary of Terms

Personal Data

“Personal data means data which relates to a living individual who can be identified from the data, or from other information which is in the possession of or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual”.

Processing

“Processing, in relation to information or data, means obtaining, recording, or holding the information or data which includes, in relation to personal data, obtaining or recording the information to be contained in the data, or carrying out any operation or set of operations on the information or data”.

Data

This means information which:

• Is being processed by automated equipment.
• Is recorded with the intention that it can processed by automated equipment.
• Is recorded as part of, or with the intention of being part of a relevant filing system.
• Does not fall within any of the above but forms part of an accessible record.

Relevant Filing System

“This means any “set” of manual data relating to individuals which are “structured”, either by reference to individuals or by reference to criteria relating to individuals, in such a way that “specific” information relating to a particular individual is “readily accessible”.

Data Subject

“A data subject is an individual who is the subject of personal data”.

Data Controller

“Data controller means a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed”.

North East Ambulance Service NHS Trust
Closed Circuit Television Policy and Code of Practice

Ref: Q.S.S.D. Version: 0001 Status: Draft Issue Date: Feb 2010
Data Processor

“A data processor is any person, (other than an employee of the data controller), who processes data on behalf of the data controller e.g. someone contracted to collect, hold and/or print documents containing personal data”.

Recipient

“Recipient, in relation to personal data, means any person to whom the data are disclosed”.

Third Party

“Third party, in relation to personal data, means any person other than (a) the data subject, (b) the data controller, or (c) any data processor. Third party does not include employees or agents of the data controller or data processor”.

33 Equality and Diversity statement

The Trust is committed to providing equality of opportunity, not only in its employment practices but also in the services for which it is responsible. As such, this document has been screened, and if necessary an Equality Impact Assessment has been carried out on this document, to identify any potential discriminatory impact. If relevant, recommendations from the assessment have been incorporated into the document and have been considered by the approving committee. The Trust also values and respects the diversity of its employees and the communities it serves. In applying this policy, the Trust will have due regard for the need to:

- Eliminate unlawful discrimination
- Promote equality of opportunity
- Provide for good relations between people of diverse groups

34 Dissemination and Implementation

34.1 Once ratified, this document shall be circulated by e-mail to all manager and locations. An article will also be placed on the Pulse to inform all staff groups.

34.2 Once ratified this policy will be added to the Document Quality Control System and added to the Intranet site to which all staff have access. Earlier versions of the document will be archived in the quality system.

34.3 Information about this policy will be added to Statutory and Mandatory Training which is delivered to all staff on an annual basis.

35 Consultation, Approval and Ratification Process

35.1 This policy has been discussed with the in representatives from staff side and all directorates.

35.2 This policy has been submitted to the Policy Review Group for approval.

35.3 This policy has been approved by the Policy Review group and submitted to the JCC for ratification.

36 Monitoring Compliance
This policy will be reviewed twelve monthly or earlier if required by:

The Trust Board
The Assurance Committee

The effectiveness of the policy will be monitored on regular basis via the Information Governance Working Group.

37  Review and Revision Arrangements including Version Control

37.1 The policy shall be reviewed at least annually by the Head Risk and Claims. The Trust Assurance Committee shall approve the Policy thereafter. All reviews and revisions to any procedural document must be approved according to the process described in section 35 of this document.

37.2 A Version Control sheet shall be maintained with the document. See Appendix M
### Appendix ‘A’ Visitor Access Log
(Control Room)

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**

Visit Authorised by:  
Position: 

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**

Visit Authorised by:  
Position: 

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**

Visit Authorised by:  
Position: 

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**

Visit Authorised by:  
Position: 

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**

Visit Authorised by:  
Position: 

<table>
<thead>
<tr>
<th>Date</th>
<th>Visitor Name</th>
<th>Company</th>
<th>Time In</th>
<th>Time Out</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Reason for Visit:**
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 North East Ambulance Service NHS Trust CCTV Policy document, which is available upon request.

The North East Ambulance Service NHS 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.
- A description of the scene where the recording took place i.e. vehicle, Trust building.
- Acceptance of the fee of £10 for the production of the images.

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 Trust’s CCTV system are not normally retained for longer than 31 days.

There is a non-refundable £10 administrative charge for your request to be considered.

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 North East Ambulance Service NHS Trust CCTV policy or contact the Trust's Head of Risk and Claims or Local Security Management Specialist.

Appendix ‘C’ Subject Access Request Form

Subject Access Request Form

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

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

Name: (Trust Data Controller)
Address: (North East Ambulance Service)

Postcode:

(Section 1) Day of Incident/Visit
Start Time of Incident/Visit:
Duration of Incident/Visit:

Date of Incident/Visit:
End Time of Incident/Visit:

(Section 2) A photograph is necessary for North East Ambulance Service to successfully identify you; therefore you should include a clear photograph of yourself. Unfortunately North East Ambulance Service can not comply with this request if a photograph is not attached.

Please provide a full description of yourself, what you were wearing, and any items you were carrying, and brief descriptions of any other people that were in your party in order to help us positively identify you.

Details:

(Section 3) In order for North East 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 North East 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. North East Ambulance Service will then endeavor to arrange a mutually convenient time and date for you to attend the Trust Headquarters and view the data.

(Tick box)

(Section 5) A fee of ten pounds (£10) is requested for all Data Access requests for administration purposes, unless you elect to view the data at the Site and vehicle. In the event of the data being viewed at the site and vehicle and you then still wish to receive a copy of this data (images/footage) then the fee will be payable.

Please make all payments payable to “North East Ambulance Service”.

(Section 6) 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 application 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 7) The CCTV System installed inside the sites, vehicles and surrounding land is operated by North East 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.

North East 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 8) 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:

North East Ambulance Service Data Controller  
North East Ambulance Service NHS Trust  
Bernicia House  
Goldcrest Way  
The Waterfront  /Newburn Riverside  
Newcastle  
NE15 8NY

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 NORTH EAST AMBULANCE SERVICE Limited (UK) 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 9) Office Use Only

Date request received:

Received by:

Action Taken:

☐ Passed to Trust Data Controller or Security Responsible.  
Date:

☐ Letter sent to subject requesting further information.  
Date:

☐ Letter sent to subject refusing access to data.
Data Protection (CCTV) Training Log

Refresher training should be conducted annually to ensure that all employees are up-to-date with changes in legislation and North East Ambulance Service's policy and code of practice.

<table>
<thead>
<tr>
<th>First name</th>
<th>Surname</th>
<th>Dept</th>
<th>Date</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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

#### Dept./Company

#### 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

#### Dept./Company

#### 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

#### Dept./Company

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

---

North East Ambulance Service NHS Trust
Closed Circuit Television Policy and Code of Practice

Ref: Q.S.S.D.  Version: 0001  Status: Draft  Issue Date: Feb 2010
Appendix ‘F’ Footage Retention Log

North East Ambulance Service NHS Trust

Footage Retention Log

Please use this log if it is deemed necessary and appropriate to retain data (images/footage) longer than outlined in the North East 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>

Authorized 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>

Authorized 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>

Authorized by: Serial/Security No:

Details: (Reason for extended retention, camera location, description of footage, etc.)
### Appendix ‘G’ 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>
</tbody>
</table>
Appendix ‘H’ Covert Surveillance Request Form

Covert Surveillance Request Form

There should be a clear and specific criminal activity identified and an assessment undertaken as to the need to use covert surveillance to obtain evidence of that criminal activity before completing this request form.

You should ensure that if equipment being used has a sound recording facility, then this should not be used to record conversations between members of the public.

Note: No installation of covert surveillance equipment should take place until this form has been completed and approved.

(Details of person requesting covert surveillance):

Name: [ ] Position: [ ]

Email: [ ] Contact No: [ ]

Site: [ ] Site No: [ ]

(Reason for request): Please provide as much detail as possible as to the reason as to why you are requesting the use of covert surveillance equipment, what evidence you already have in connection to this investigation/incident, and what you expect to achieve from utilizing this type of equipment.

Details:
(Time Frames): If an extension of this time frame is required then a new form needs to be completed and authorised by the UK Risk Manager or in their absence, their deputy.

Start Date/Time:  End Date/Time:

(Authorisation): If authorisation has been confirmed by fax/memo then this must be affixed to the request form and retained for evidential purposes.

Head of Risk and Claims:

<table>
<thead>
<tr>
<th>Forename</th>
<th>Surname</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>

Security Management Director

<table>
<thead>
<tr>
<th>Forename</th>
<th>Surname</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
</table>

Appendix 'I' Investigation Observation Log

<table>
<thead>
<tr>
<th>Date</th>
<th>Time (Start / End)</th>
<th>Observation Details</th>
<th>Observer Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

North East Ambulance Service NHS Trust

Investigation Observation Log

This form should be used to log all observations undertaken in support of any investigation of possible criminal activity or equivalent malpractice (including breaches of company policy and procedures).
Appendix ‘J’ CCTV Certificate of Training

North East Ambulance Service NHS Trust

This is to certify that

__________________________________________

has received training in

CCTV
(Data Protection Procedures)

and has covered the following subjects:

- Data Protection (8 Principals)
- Protection of CCTV System
- Access to the CCTV Control Room and Vehicle Systems
- Monitoring Procedures
- Covert Surveillance
- Recording Material (Digital/Analogue)
- Retaining Information
- Access to Images
Appendix ‘K’ Approved Persons to Access/Maintain CCTV System

Head of Risk and Claims – access to all systems
Local Security Management Specialist – access to all systems
HART Manager – access to HART CCTV systems only
### Appendix ‘L’ Access to View or Copy Images – Police

<table>
<thead>
<tr>
<th>Name of person making request</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of Request</th>
<th>Time of Request</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Police Collar Number (if applicable)</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Office Tele Number</th>
<th>Mobile Tele Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Details of Image to be Viewed

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reason (For police only)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>
## To be Completed if Images are Removed

<table>
<thead>
<tr>
<th>Ref. No.</th>
<th>Crime No: (For Police Only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issued To</td>
<td>Police Collar Number</td>
</tr>
<tr>
<td>Issued By</td>
<td>Date Issued</td>
</tr>
</tbody>
</table>

| Details of Images Removed |

---

I acknowledge receipt of the above CD(s)

| Signed | Date | Return Date |

## Appendix M - Version Control Sheet

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
</table>

---

North East Ambulance Service NHS Trust
Closed Circuit Television Policy and Code of Practice

Ref: Q.S.S.D.       Version: 0001       Status: Draft       Issue Date: Feb 2010