Closed circuit television (CCTV) policy

DOCUMENT INFORMATION	
Author:	Callum Johnston
Date of Issue:	June 2018
Review due by:	June 2021
Version:	**V1**

Contents

1. Introduction 4
2. Scope 4
3. Equality statement 4
4. Aim 4
5. Roles and Responsibilities 5
   5.1 Company Board 5
   5.2 Chief Executive 5
   5.3 Executive Director 6
   5.4 Director of Patient Care and Service Transformation ..... **Error! Bookmark not defined.**
   5.5 Managers and Supervisors 6
   5.6 All staff 7
   5.7 Local Security Management Specialists/Risk Team ..... **Error! Bookmark not defined.**
   5.8 Head of Estates ..... **Error! Bookmark not defined.**
   5.9 Driving Standards Manager 7
   5.10 Information Governance Manager 7
   5.11 Head of Resilience and Specialist Operations . **Error! Bookmark not defined.**
   5.12 Driving Education Department ..... **Error! Bookmark not defined.**
   5.13 South Central Fleet Services Ltd ..... **Error! Bookmark not defined.**
6. Types of CCTV recording systems in use within the Company 8
7. The purpose of the Company's CCTV recording systems and the use of images captured by these systems 8
8. CCTV recording systems in the saloons of vehicles 9
9. Access to the Company's CCTV recording systems and recorded images 10
10. Storage, security and maintenance of the recording systems in Company vehicles 16 12
   10.1 Retention of Images captured by the Company's CCTV recording systems 13
11. CCTV Signage at Company premises and in Company vehicles 13
12. Compliance with the principles of the Data Protection Act and offences under the DPA 14
13. Use of CCTV images in connection with disciplinary procedure 14
   14. Use of CCTV images in connection with Clinical negligence 14
   15. Staff being filmed by Members of the Public (MOP) in a public place 14
16. Training 15
17. Equality and Diversity 15
18. Monitoring 15
19. Consultation and Review 16
20. Implementation (including raising awareness) 16
21. References 16
22. Associated documentation ..... **Error! Bookmark not defined.**
23. Appendix 1: Review Table 17
24. Appendix 2 17
25. Appendix 3 18
26. Appendix 4: The current agreement between SCAS and SCFS Ltd with regards to the servicing and maintenance of the VDR8 system ..... **Error! Bookmark not defined.**

27. Appendix 5..... 19
28. Appendix 5 : Responsibility Matrix – Policies, Procedures and Strategies .. **Error! Bookmark not defined.**
29. Appendix 5 : Equality Impact Assessment Form Section One – Screening..... 22
30. : Equality Impact Assessment Form Section Two – Full .. **Error! Bookmark not defined.**
Assessment .....**Error! Bookmark not defined.**
31. : Ratification Checklist .....**Error! Bookmark not defined.**

1. Introduction

1.1 The Company recognises its responsibilities under the Data Protection Act (DPA) 1998 and the associated data protection principles with regard to the use and operation of Close circuit television (CCTV) recording systems within the Company.

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

2. Scope

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

3. Equality statement

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

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

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

4. Aim

4.1 The aim of this policy is to set out the arrangements the Company has in place with regards the use, operation and management of the CCTV systems in its premises and vehicles. It is also to ensure that the use, operation and management of the CCTV systems in Company premises and vehicles and any images captured and recorded by these systems complies with the Data Protection Act 1998 and all other relevant legislation concerning CCTV.

4.2 The policy also aims to ensure that:

- the use and operation of the CCTV within the Company is for assisting with the maintaining of the security of Company premises and vehicles; for preventing and investigating crime; assisting with the protection of staff; and assisting with the investigation of incidents involving:

  - staff being subject to abuse, or threatened or assaulted in the saloon of the vehicle;
  - and/or road traffic collisions involving Company vehicles
  - and/or complaints

- all access, retrieval, viewing and use of the CCTV and any images captured is done in accordance with the Data Protection Act 1998 and its principles and any other relevant legislation
- the sharing of any information captured by the CCTV is done in accordance with the Data Protection Act 1998
- any images recorded are not to be used as part of any disciplinary procedure or in connection with any alleged clinical negligence against a member of staff unless they are in breach of section 7 of this policy. (Where an investigation take place, the member of staff involved has the right to request and review the images captured by the Company's CCTV recording systems)
- all of the images recorded and information captured by CCTV is held, secured and disposed of in accordance with the Data Protection Act 1998.

5. Roles and Responsibilities

5.1 Company Board

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

5.1.2 It will also ensure that there are suitable and sufficient arrangements for the management of health and safety and the identification, assessment and management and control of risks to patients, staff, the general public (anyone affected by the activities of the Company),

5.2 Managing Director

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

5.2.2 He is also responsible for ensuring that:

- Company policies are reviewed as appropriate in order to secure continuing compliance with existing policies, current legislation and any changes in the law

- the allocation of the resources necessary to maintain sound and efficient health and safety and security arrangements
- the effective implementation of this policy within the Company and for ensuring that there are suitable and sufficient arrangements for the identification, assessment and management and control of the risks.

5.3 Clinical Director

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

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

5.4 Managers and Supervisors

5.4.1 All Managers and Supervisors are responsible for:

- following any relevant guidance issued on the CCTV within the Company and the Data Protection Act 1998
- attending any training to enable them to fulfil their responsibilities outlined in this policy
- bring this policy to the attention of staff within their areas of responsibility
- ensuring that all staff within their area of responsibility comply with this policy and any associated protocols and procedures
- ensuring that all incidents involving a breach of security on Company premises are reported on the Company's Incident reporting systems, CASUS.
- encouraging staff to report all incidents involving an activation of the CCTV systems within the Company using the Company's Incident reporting system, CASUS
- ensuring that members of staff are given support following an activation of the CCTV as a result of a violence and aggression incident and/or a road traffic collision
- investigating, and/or arranging for the investigation of incidents following the activation of the CCTV and which involve their staff
- where necessary, seeking advice on the use and operation of CCTV within the Company
- where necessary, referring any staff who have activated CCTV as a result of being subject to violence and aggression and/or a road traffic collision
- assisting with the development of a pro-security culture within the Company.

5.5 All staff

5.5.1 All staff have the following responsibilities:

- to make themselves fully aware of this policy and abide by it
- to take reasonable care for their health and safety and that of others who may be affected by their acts or omissions
- to abide by any information, instruction and guidance provided to them in the use and safe operation of the Company's CCTV system
- to adhere to any safety measures put in place to ensure their safety, including any safe systems of work or safe operating procedures in relation to the Company's CCTV system
- to activate the internal CCTV in Company vehicles whenever it is necessary
- to report any activation of the CCTV system in/on Company vehicles using the Company's Incident reporting system, CASUS
- to report any breaches of the use of the CCTV system and the Data Protection Act 1998 using the Company's Incident reporting system, CASUS
- to report all incidents involving a breach of security on Company premises and vehicles
- to report any incidents involving being filmed by members of the public using the Company's incident reporting system, CASUS
- to comply with the Data Protection Act 1998 and CCTV Code of Practice
- where necessary, provide the Police with statements
- to assist with the development of a pro-security culture within the Company

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

5.6 Driving Standards Manager

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

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

5.7 Information Governance Manager

5.7.1 The Information Governance Manager is responsible for:

- ensuring that the Company is registered for the use and operation of close circuit television systems with the Information Commissioner's Office as per the Data Protection Act 1998
- for dealing with requests from Company Investigators, the Police and members of the public and other Third parties for access to and obtaining images captured by the Company's CCTV recording systems

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

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

6.0.2 The use of CCTV recording systems in the Company is subject to the requirements of the Data Protection Act 1998 and as such needs to comply with Data Protection Principles, see section 11.

6.0.3 The Company is registered to operate CCTV cameras under the Data Protection Act 1998.

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

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

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

6.2 CCTV recording systems installed in Company vehicles

6.2.1 Company vehicles have CCTV installed in them and there are cameras located on the outside of vehicles and also in the saloon of the vehicle. The CCTV recording systems consist of either a hard drive system or a flash card system. For further information on the CCTV recording systems in/on Company vehicles see section 7 below.

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

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

- maintaining the security of premises, vehicles and assets by assisting with the protection of premises, vehicles and assets
- detecting, preventing and investigating incidents of theft of, or damage to, Company property and assets
- protecting staff
- investigating incidents involving abuse and threats to Company staff and others involved in Company work
- investigating attempted or actual assault of Company staff and others involved in Company work in the saloon of Company vehicles
- investigating road traffic collisions (RTCs)/Ambulance vehicle incidents (AVI) and road traffic incidents/complaints which involve Company vehicles.

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

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

8. CCTV recording systems in the saloons of vehicles

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

- A hard disk system is installed in the vehicles which, once activated, will record from five seconds before the panic strip is pressed and for the remainder of the recording. The recorded footage is held for three weeks before being overwritten.

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

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

8.1.2 If a saloon activation of an actual or potential incident has taken place the member of staff who activated the CCTV recording system must contact the Duty manager They must also report the incident using the Company's incident reporting system, CASUS.

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

8.2.1 Following the reporting of an incident involving the activation of the internal cameras in the saloon of a Company vehicle, and/or following the retrieval of a request of any images captured, a member of the managment Team will arrange for the removal of the hard drive and store this in a secure place.

8.2.2 On removal of the hard drive for viewing purposes or use in legal proceedings the member of the managment Team will ensure the following is documented and recorded on the associated incident report form on CASUS:

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

8.3 CCTV Recording systems on the exteriors of vehicles

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

- front, rear and side facing cameras installed which continuously record, whilst powered up. Recordings will be held on the hard drive for approximately four weeks before being overwritten.

8.3.2 The recordings of images from external cameras are stored on the same device as the interior saloon cameras.

8.4 Activation of the external CCTV cameras on vehicles

8.4.1 If a Company Ambulance or rapid response vehicle collides with or is involved in a road traffic incident with another vehicle or is obstructed by another vehicle then the CCTV recording system will record and capture images leading up to the said incident and the incident. Once the ignition on these vehicles is turned on, the external cameras are activated and recording.

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

8.5 Retrieving information from external cameras following a road traffic incident

8.5.1 As part of the ensuing investigation process following a road traffic collision (RTC)/Ambulance vehicle incident (AVI) and/or road traffic incident/complaint, the following information will be recorded and may be included within the Investigation Report if deemed relevant by the Driving Standards Department: See Appendix 4for Driving Standards form.

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

8.5.2 Where necessary, Driving Standards may share footage from road traffic incidents/AVI with the Company's Motor Insurance Company. This may be done by utilising an i-cloud.

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

9.0.1 Access to the Company's CCTV recording systems and recorded images will only take place in accordance with this policy. Therefore, only authorised personnel as stated

in appendix 2 will have access to the CCTV recording systems in Company vehicles and premises.

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

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

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

9.1.2 Once the request has been received, the Information Governance Manager will liaise with the clinical manager/Driving Standards Manager to retrieve the footage from the Company's CCTV recording systems.

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

9.2.1 Under the Police and Criminal Evidence Act (PACE) 1984, the Police may apply to the Company for access to hard drives or recorded images taken from the Company's CCTV recording systems where they reasonably believe that these hard drives/flash cards have captured images that will assist with their investigation and detection of crime and/or the prevention of crime.

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

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

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

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

9.2.5 When a request is made by the Police to obtain a copy of the hard drive a verified copy of the hard drive will be provided to them and the Company will retain the original hard drive.

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

9.3 Requests from the public to access CCTV images

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

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

9.3.3 The Information Governance Manager will be responsible for considering any such requests in accordance with the Data Protection Act 1998 and the CCTV Code of Practice issued by the Information Commissioner's Office and in compliance with this policy.

9.3.4 Once the Information Governance Manager has received a request and is satisfied that the request is in order and can be responded to,

9.3.5), the response should be disclosed as soon as reasonably possible. . In accordance with the Data Protection Act 1998, the time frame for replying to Data Protection Subject Access requests is one month; however the company aims to respond within 21 days. This time frame begins from the initial receipt of the request and may only be halted if clarification of the request or payment is sought.

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

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

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

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

9.3.9 Where the requester who made the Subject Access request wishes to view the images on the Company's premises, this should be done in a secure location with only the relevant Company personnel and the requester present.

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

9.4 Other Third party access to recorded images/data

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

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

10.0.1 Following retrieval, each hard drive will be secured in a locked cupboard. This will deter or prevent tampering with or unauthorised viewing of their contents and make any such tampering evident.

10.0.2 Any hard drive or duplicate hard drive which is supplied to an approved third party must be kept in a secure location.

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

10.1.1 CCTV images should be stored and treated in the same manner with the same security and confidentiality of electronic and manual records. CCTV images should be stored within a lockable cupboard to prevent unauthorised access.

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

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

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

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

- Hard Drives which have automatic overwriting facilities should be activated so that the material/images is removed;
- Images that have been printed off as a still shot, should be shredded and disposed of in confidential manner;
- CCTV that has been put onto a disc should be shredded using a shredder that has the facilities for this.

10.2 Removal of CCTV recording systems

10.2.1 When the CCTV recording systems in a Company premises or vehicle are obsolete and it is being dismantled and removed then in accordance with the Data Protection Act 1998 the hard drives of these systems must be removed and all images on the hard drive must be wiped clean and removed and a check must be carried out to ensure that this has been done.

11. CCTV Signage at Company premises and in Company vehicles

11.0.1 To assist with the Company in complying with the Data Protection Act 1998, appropriate signage informing the public that CCTV is in operation shall be displayed at those Company premises and vehicles where CCTV recording systems have been installed.

11.0.2 The signage will be displayed on the external façade of Company buildings and/or at the perimeter of the area covered by the CCTV. The signage will state display details of the organisation who is operating the system, namely,Leicester Event Medical LTD. It should also display the contact details for any enquires or complaints.

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

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

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

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

12.1 The Company has to comply with the principles of the Data Protection Act 1998 which are that personal information shall:

- be fairly and lawfully processed
- be processed for limited purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be kept for longer than is necessary
- be processed in accordance with the data subject's rights
- be kept secure
- not to be transferred to countries without adequate protection.

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

12.3 The Data Protection Act 1998 also provides for separate liability for offences in the Act of Directors or other senior management of the Company who have committed the offence.

13. Use of CCTV images in connection with disciplinary procedure

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

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

14. Use of CCTV images in connection with Clinical negligence

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

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

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

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

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

16. Training

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

16.2 Training in the usage and retrieving of CCTV images will be given when required.

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

17. Equality and Diversity

17.1 An equality and diversity impact assessment has been carried out on this policy and can be found at Appendix 5 .

18. Monitoring

18.1 The effectiveness of this policy will be monitored in the following way.

Standard / process / issue	Monitoring and audit			
	Method	By	Committee	Frequency
a) The number of download of the CCTV in Company premises. b) The number of downloads of the CCTV in the saloon of Company vehicles. c) The number of downloads of CCTV on the exterior of Company vehicles.	a) Annual report on these downloads of the CCTV in Company premises. b) Annual report on these downloads of the CCTV in saloon of Company vehicles. c) Annual report on the downloads of the CCTV on the exterior of Company vehicles. d) 10% annually	a) Head of Estates b) Head of Risk and Security c) Driving Standards Manager. d) Assistant Director of Operations and Support Services.	a) Health, Safety and Risk Group.	a) Annually. b) Annually. c) Annually. d) Annually.

19. Consultation and Review

19.1 A consultation exercise on the policy will be carried out with the stakeholders listed below.

19.2 This policy will be reviewed every three years or whenever there are changes to the relevant legislation.

Stakeholder or Group Title	Consultation Period (From-to)	Comments received (Yes/No)

20. Implementation (including raising awareness)

20.1 The policy will be implemented and communicated to managers and staff within the Company via the weekly newsletter, Staff Matters.

21. References

- Health and Safety at Work etc. Act 1974
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- Criminal Procedure and Investigations Act 1996
- Protection from Harassment Act 1997
- Human Rights Act 1998
- Data Protection Act 1998
- General Data Protection Regulations 2018
- Regulation of Investigatory Powers Act (RIPA) 2000
- Freedom of Information Act 2000
- Home Office CCTV Operational Requirements Manual 2009
- Home Office Surveillance Camera Code of Practice 2013
- Home Office UK Police requirements for digital CCTV systems
- Information Commissioners Office (ICO) In the picture: A data protection code of practice for surveillance cameras and personal information 2014
- Data Protection (Assessments Notices) (Designation of National Health Service Bodies) Order 2014
- Information Commissioners Office (ICO) Privacy Impact Assessment (PIA)
- NHS Protect Closed Circuit Television
- Surveillance Camera Commissioner Code of Practice: A guide to the 12 principles of surveillance
- Secretary of State's Directions on Security Management Measures (March 2004)

23. Appendix 1: Review Table

Version	Reason for change	Overview of change

24. Appendix 2

AUTHORISED PERSONS TO ACCESS OR MAINTAIN CCTV SYSTEMS

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

- Managing Director
- Clinical Director
- Information Governance Manager
- Driving Standards Manager

25. Appendix 3

CCTV SUBJECT ACCESS INFORMATION

(Draft letter)

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 Leicester Event Medical LTD CCTV Policy document, which is available upon request.

Leicester Event Medical LTD will accept requests made for Personal Data under the Data Protection Act. Such requests may be made in writing to the Company. All requests for personal images contained on CCTV must include:

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

All requests will be dealt with in accordance with 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 Company's CCTV system are not normally retained for longer than 40 days.

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

Any request will receive an initial reply within one month.

For further information please ask for a copy of Leicester Event Medical LTD CCTV policy or contact the Company Information Governance Manager.

27. Appendix 4

DRIVING STANDARDS DEPARTMENT

INCIDENT DATA RECORDER / IMAGE RECORDING INFORMATION SYSTEM DOWNLOAD FORM

Incident Data Recorder (IDR) ☐ Image Recording Information System (IRIS) ☐

IDR Download to be stored as follows; Reg no, Odometer reading (indicate miles or kms), Date, Clock set (Y/N) Initials.
eg. ***RX05NUE 24670M 191211 Y JWP***

Download Information	
Download Reference no	
UDS Identification number	
Reg No and Fleet ID	
Date / Time	
Downloaded at	
Vehicle make / model	
Comments:	

Download to be passed to

Name	
Organisation	
Date received	
Signed as received	
Reason for requiring download (must include authorising LEM Director details)	

The information from this activity has been stored and access to it may be granted by using the procedure within the Company's Circuit Television (CCTV) Policy.

The above information and download have been extracted and stored in line with the Companys

Closed Circuit Television (CCTV) Policy.

Signed…….. Print……..……...

29. Appendix 5 : Equality Impact Assessment Form Section One – Screening

Name of Function, Policy or Strategy: Close circuit television (CCTV) Policy.

Officer completing assessment: Callum Johnston, Managing Director.

Telephone: 0116 216 6949.

1. What is the main purpose of the strategy, function or policy?
The aim of this policy is to set out the arrangements the Company has in place with regards the use, operation and management of the CCTV systems in its premises and vehicles. It is also to ensure that the use, operation and management of the CCTV systems in Company premises and vehicles and any images captured and recorded by these systems complies with the Data Protection Act 1998 and all other relevant legislation concerning CCTV.
2. List the main activities of the function or policy? (for strategies list the main policy areas)
The policy also aims to ensure that: • the use and operation of the CCTV within the Company is for assisting with the maintaining of the security of Company premises and vehicles; for preventing and investigating crime; assisting with the protection of staff; and assisting with the investigation of incidents involving: ➢ staff being subject to abuse, or threatened or assaulted in the saloon of the vehicle; ➢ and/or road traffic collisions involving Company vehicles • all access, retrieval, viewing and use of the CCTV and any images captured is done in accordance with the Data Protection Act 1998 and its principles and any other relevant legislation • the sharing of any information captured by the CCTV is done in accordance with the Data Protection Act 1998 • any images recorded are not used as part of any disciplinary procedure or in connection with any alleged clinical negligence against a member of staff unless they are in breach of section 7 of this policy • all of the images recorded and information captured by CCTV is held, secured and disposed of in accordance with the Data Protection Act 1998.
3. Who will be the main beneficiaries of the strategy/function/policy?
All who work in or for the Company.

1. Use the table overleaf to indicate the following:- a. Where do you think that the strategy/function/policy could have an adverse impact on any equality group, i.e. it could disadvantage them? b. Where do you think that there could be a positive impact on any of the groups or contribute to promoting equality, equal opportunities or improving relations within equality target groups?

		Positive Impact	Negative Impact	Reasons
GENDER	Women	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	Men	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
RACE	Asian or Asian British People	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	Black or Black British People	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	Chinese people and other people	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	People of Mixed Race	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	White people (including Irish people)	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
DISABILITY	Disabled People	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
SEXUAL ORIENTATION	Lesbians, gay men and bisexuals	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
AGE	Older People (60+)	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.

	Younger People (17 to 25) and children	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.

RELIGION/BELIEF	Faith Groups	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.
	Equal Opportunities and/or improved relations	✓		Policy is designed to protect staff and people who carry out work for or on behalf of the Company.

Notes:

Faith groups cover a wide range of groupings, the most common of which are Muslims, Buddhists, Jews, Christians, Sikhs and Hindus. Consider faith categories individually and collectively when considering positive and negative impacts.

The categories used in the race section refer to those used in the 2001 Census. Consideration should be given to the specific communities within the broad categories such as Bangladeshi people and to the needs of other communities that do not appear as separate categories in the Census, for example, Polish.

5. If you have indicated that there is a negative impact, is that impact:		
	Yes	**No**
Legal (it is not discriminatory under anti-discriminatory law)		✓
Intended		✓
Level of Impact	**High**	**Low**
If the negative impact is possibly discriminatory and not inte please complete a thorough assessment after completing the		✓
6(a). Could you minimise or remove any negative impact that is of low significance? Explain how below:		
6(b). Could you improve the strategy, function or policy positive impact? Explain how below:		
7. If there is no evidence that the strategy, function or policy promotes equality, equal opportunities or improves relations – could it be adopted so it does? How		
Please sign and date this form, keep one copy and send one copy to the Company's Equality Lead.		
Signed:……		
Name: c johnston.		
Date: 20th June 2018.		