East London
NHS Foundation Trust

Closed Circuit Television Policy

Version number :	1.0
Consultation Groups	Estates and Facilities, Information Governance, Lead Nurses
Approved by (Sponsor Group)	Health, Safety & Security Committee
Ratified by:	Quality Committee
Date ratified:	May 2020
Name of originator/author:	Day Njovana, Associate Director of Safety and Security – forensics , Richard Harwin, Health, Safety, Security and Emergency Planning Manager (LSMS)
Executive Director lead :	Lorraine Sunduza
Implementation Date :	May 2020
Last Review Date	May 2020
Next Review date:	June 2023

Services	Applicable
Trustwide	X
Mental Health and LD	
Community Health Services	

East London
NHS Foundation Trust

Version Control Summary

Version	Date	Status	Comments/ Changes
1.0	June 2020	Final	New Policy- separated from Security Policy

Contents

Page No:	
1	Introduction
1	Rationale
2	Purpose and Outcome
3	Roles and Responsibilities
5	Systems and Recording
6	CCTV Surveillance Scheme Standards
10	Disposal of Recorded Images / Documentation
10	Guidance on the Use of CCTV During Internal Investigations
12	Complaints Procedure
12	Training
12	Monitoring / Review
13	References / Supporting Documents
14	Appendix 1 – CCTV Flow Chart
15	Appendix 2 Form - Application for Trust Managers to View Recorded Images
17	Appendix 3 Form - Application for Trust Managers to Receive a Copy of Recorded Images
19	Appendix 4 Form – Application for Access to Recorded Images (Subject Access Request)

Executive Summary

- The CCTV Policy outlines the responsibilities the trust has to its employees, visitors and patients and external organisations.

- Provide and maintain a working environment that is safe, secure and free from the dangers of crime for all people who may be affected by its activities so that health care is delivered with minimum disruption.

- CCTV accountability lies with the Trust Board and there is both a nominated executive and non-executive director responsible for security issues.

- The trust has a Local Security Management Specialist (LSMS) in post to oversee CCTV requirements.

- The policy will ensure requirements and recommendations will be monitored by the trust Quality Committee.

1. INTRODUCTION

1.1 This policy describes the arrangements for the management of overt Closed Circuit Television (CCTV) surveillance on Trust premises. It should be read in conjunction with 'In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information' (2017) issued by the Information Commissioner's Office. Copies of the Code of Practice can be sourced on the internet. Compliance with this policy will ensure compliance with the requirements of the Data Protection Act (2018), as applied to the use of CCTV, and the General Data Protection Regulations (GDPR).

1.2 All overt CCTV surveillance schemes shall be operated for the purposes of helping to maintain safety and security.

1.3 The Trust is committed to providing a safe place of work. To this end this policy is designed to introduce proactive procedures that will ensure, so far as is reasonable practicable, not only the health and safety of its staff but also its welfare in terms of security.

2. SCOPE

2.1 The CCTV policy applies to all employees (including those on permanent, temporary and bank contracts), holders of ELFT honorary contracts and secondees to ELFT. For the purposes of this policy, all the aforementioned will be referred to as 'employees'.

2.2 Staff, patients and visitors of East London Foundation NHS Trust have the right to be confident that they are safe and their personal property is secure. In addition to making continuous improvements to achieve this, the Trusts buildings and property will be sufficiently protected so that the highest possible levels of clinical care, so far as is reasonably practicable, may be delivered in our person focused service.

3. RATIONALE

3.1 East London NHS Foundation Trust, hereafter referred to as 'the Trust' is committed to providing a safe and secure environment for staff, patients and visitors. This is framed by National and European Health & Safety Legislation, the Department of Health and the NHS Counter Fraud Authority.

3.2 The Trust Board recognises that security management is an integral part of good, effective and efficient risk management practise and to be effective should become part of the Trust's cultural and strategic direction.

3.3 The Board is therefore committed to making sure that security management forms a vital part of its philosophy and business plans rather than being viewed or practised as a separate programme; ensuring that responsibility for implementation is accepted at all levels of the organisation.

4. PURPOSE AND OUTCOME

4.1 Safeguarding the Trust's property, assets and private property against crime is of paramount importance. The principles are:

- The protection of life from malicious activity or other hazards.
- The prevention of the loss of Trust property and assets as a result of crime.
- The protection of Trust property against malicious acts, theft, criminal damage, and trespass.
- The preservation of good order within the premises under the Trust's control.
- The detection and reporting of suspected offenders who are committing offences against Trust staff, property or private property within the Trust's premises.

4.2 The purpose of this policy is to declare what needs to be done, by whom and by when to ensure that:

- Every opportunity is taken to reduce the chances of a security incident arising in the first place.
- In the event of a security incident occurring it is handled properly to help reduce its severity and in particular to minimise the risk of any personal injury or damage/loss of property.
- Steps are taken to minimise any lasting effect of incidents particularly regarding personal counselling and restoration of services etc.

4.3 The Trust recognises the potential effects of security incidents on the morale, retention and efficiency of staff and that the public image and competence of the organisation may be affected by the occurrence of serious untoward incidents. By implementing seven generic areas of action to tackle security breaches the Trust will appreciate a pro-security culture by operating to the national standards set out by the NHS Counter Fraud Authority.

There are seven generic areas of action with which to build a pro-security culture:

- Prevention
- Deterrence
- Investigation
- Detection
- Sanction
- Redress

4.4 This policy has been developed in light of currently available information, guidance and legislation that may be subject to review.

The Quality Committee will review this policy and any recommendations for change will be submitted to the Quality Committee. The Quality Committee will also monitor to ensure that all the recommendations and the processes outlines in this policy are complied with.

5. ROLES AND RESPONSIBILITIES

5.1 Chief Executive

The Chief Executive has the overall statutory responsibility for security management within the Trust

5.2 Trust Board

Directors on behalf of the Chief Executive are responsible for ensuring that the Trust's Security Policy is implemented within the organisation. This will include responsibility for:

•Promoting a pro-security culture.

•Planning the capital investment required to address matters arising from risk assessments.

•Ensuring that security risk assessments are undertaken within their areas, working in conjunction with the Trust's Security Management Director (SMD) and Local Security Management Specialist.

•Ensuring that staff for whom they are responsible are aware of identified security risks and that they receive appropriate training.

•Taking appropriate action in respect of persons suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the Trust, falling in line with the 7 generic areas of action (section 4).

•Ensuring staff awareness of this policy.

•Ensuring that security arrangements within their Directorate are being observed and any deficiencies are reported.

•Ensuring that every member of staff obtains a Trust security identity (ID) card and that it is worn and visible at all times whilst the staff member is on Trust premises or undertaking Trust business in other premises.

•An ongoing commitment to staff training.

•The Chief Nurse is the Board Director responsible for ensuring that the Trust has suitable and sufficient measures in place to ensure the security of its staff, clients, property and assets.

5.3 Security Management Director (SMD)

As the Board member responsible for security, the Chief Nurse has specific responsibilities to ensure that security arrangements are adequate and ensuring that the Trust has suitable and sufficient measures in place to ensure the security of its staff, clients, property and assets.

•Ensure compliance with the Secretary of State directions, as amended in 2004. For convenience these will be referred to as "directions/directives".

•Formulation, implementation and maintenance of an effective Security Management Policy.

•To review and amend this policy to ensure compliance with any current legislation, or directions issued by the NHS Counter Fraud Authority.

•Ensuring that all provisions of the CCTV sections of the Data Protection Act are complied with and all systems are registered with the relevant Data Protection Authorities.

•Monitoring the performance of the Trust and Directorates with regard to the implementation of this policy.

5.4 Trust Directors

Directors will support the Chief Executive and carry direct responsibility for the implementation of this policy in their directorate, and to ensure that their managers undertake compliance spot checks on a regular basis**.**

5.5 Local Security Management Specialist/Health, Safety & Security Manager

At least one Local Security Management Specialist should be nominated to the Trust as required by the Secretary of State Directions for Security Management.

•Provide crime prevention advice, support and assistance in upholding and developing all operational arrangements that affect security.

•Act as the focal point for contact with external agencies with security matters affecting the Trust.

•Ensure the effective management of all procedures affecting security.

•Look into all security incidents and keeps proper records.

•Provide support to staff involved in a security incident.

•Liaise with external agencies regarding security matters, such as: Police, Local Authorities etc.

•To develop and implement an effective Security Management Policy for the Trust.

•Carry out criminal investigations of any breaches or suspected breaches of security and to liaise with the Police where criminal proceedings are being considered.

•Ensure security risk assessments and crime reduction surveys are conducted in all Trust Properties.

•Assist Managers in identifying any security associated risks following a breach or suspected breach in security.

•Advise the SMD of any impacts resulting from new legislation or national directions and guidance.

•Complete a written work plan for each financial year in conjunction with the SMD.

•Complete at least one written report at the end of each financial year summarising their work for that year.

•To ensure that appropriate security advice is provided to capital schemes and Trust projects.

•Manage contract security staff engaged in duties at Trust properties and regularly liaise with the security contractor to ensure strict adherence to the terms of the contract.

•Conduct regular training for staff and organise security awareness campaigns, to highlight the importance of security and the responsibilities of all staff.

•Direct a multi-agency approach to tackle security breaches and highlighted risks.

•Attend Trust Committee and Group meetings where membership is agreed.

5.6 System Managers

For each CCTV system there must be an operational policy in place that identifies the system manager. The system managers (usually Heads of Department, Ward Managers, etc.) are managerially accountable for the scheme, staff training in the procedures and the security and disclosure arrangements

5.7 System Operators

All staff who are involved in the operation of CCTV systems are responsible for ensuring they have read, understood and comply with this policy and associated documents (see references) and for ensuring, in conjunction with the relevant system manager that they have received appropriate training for their role.

6. SYSTEMS AND RECORDINGS

6.1 The recording medium must be securely stored when not in use. It is the policy of the Trust that recordings will not normally be kept for longer than one month before they are erased. The operational policy for each CCTV System must detail the length of time that recordings will be kept.

6.2 If recordings are to be kept for longer than one month (e.g. for evidential purposes, or for use in training), the reasons must be documented and agreed by the Director of the Service.

7. CCTV SURVEILLANCE SCHEME STANDARDS

7.1 For each CCTV surveillance scheme, the Director with management responsibility for its operation will ensure that there is a documented procedure within its Departmental Operational Policies covering the standards detailed within the Code of Practice issued by the Information Commissioner. Detailed below are some of the main principles that must be incorporated within the procedure. The LSMS must be consulted regarding operational requirements for new or replacement CCTV systems.

7.2 Assessment Procedures:

- The purpose(s) of any CCTV installation must be consistent with the circumstances listed in Article 8 of the European Convention on Human Rights:
- National Security
- Public Safety
- Economic Wellbeing of the Country
- The Prevention of Disorder and Crime
- The Protection of Health or Morals or the Protection of the Rights and Freedoms of Others

The use of CCTV in ward areas must be given particularly careful consideration in terms of the extent to which it is necessary for safety and security purposes, balanced against the level of interference with the individual's privacy which it would involve.

7.2.1 Before installing and using CCTV surveillance equipment, the department responsible for operating the scheme must establish and document the purpose or purposes for which they intend to use the equipment. This documentation (i.e. Operational Policy) must also identify who is managerially accountable for the scheme, staff training in the procedures and the security and disclosure arrangements (i.e. a System Manager). The responsible Head of Service/ Borough Director must ensure that the Trust's Data Protection Officer is notified of the scheme in order that she may in turn notify the Office of the Information Commissioner.

7.3 Siting the Cameras

7.3.1 The CCTV equipment must be sited in such a way that it only monitors those spaces which are intended to be covered. Operators must be aware of the purpose for which the scheme has been established and that it must not be used for any other purpose. If cameras are adjustable by the Operators, they must be restricted so that Operators cannot adjust them to overlook spaces that are not intended to be covered by the scheme. If this is not possible, then Operators must be trained in recognising the privacy implications of such spaces being covered. In ward areas, cameras must be positioned so that they do not intrude into patients' rooms.

7.3.2 When planning a CCTV installation, it may be helpful to refer to the 'CCTV Operational Requirements Manual' (Home Office Scientific Development Branch– 2009)

7.3.3 Signs must be displayed so that persons are aware that they are entering an area which is covered by surveillance equipment. The signs must be clearly visible and legible and contain the following information:

- Identity of the organisation responsible for the scheme i.e. the East London NHS Trust. If the CCTV is operated by an external provider, the name of that organisation must be shown
- The purpose of the scheme e.g. to help maintain the safety of patients, visitors.
- Details of whom to contact regarding the scheme and a telephone number
- i.e. for further information contact the Service Director via the Trust 02076554000

7.4 Quality of the Images

7.4.1 The images produced by the equipment must be as clear as possible in order that they are effective for the purpose intended. It is the responsibility of the System Manager to ensure that upon installation and at routine intervals thereafter the equipment is checked to ensure that it performs properly.

7.4.2 The medium on which the images have been recorded must be cleaned so that images are not recorded on top of images recorded previously.

7.4.3 If recording equipment is being used this must record the location of the camera, the date and time. The System Manager must ensure these features are checked regularly to ensure they are accurate and the checks must be documented in a system logbook.

7.5 Processing the Images

7.5.1 On removing recordings which have been identified for use in legal / disciplinary proceedings or Trust Inquiries, the System Manager must ensure that they have documented:

•Any crime incident number to which the images refer.

•The location of the images.

•The signature of the collecting police / Trust officer

7.5.2 Monitors displaying images must not be viewed by anyone other than authorised persons who normally will be the System Manager and System Operators.

7.5.3 The System Manager must control access to recorded images. (S)he must only allow requests for access by third parties including other Hospital staff if they are in accordance with documented disclosure policies.

7.5.4 Viewing of the recorded images must take place in a restricted area. No other employees should be allowed access to the area where the viewing is taking place.

7.5.5 Removal of the medium on which the images are recorded, for viewing persons, must be documented as follows:

•The date and time of removal.

•The name of the person removing the images.

•The name(s) of the person(s) viewing the images. If a third party is involved, the name of the person(s) and the name of the organisation of that third party must be documented. The outcome, if any, of the viewing.

•The date and time the images were returned to the system or secure storage, and if they are to be retained for evidential purposes

7.6 Access to and Disclosure of Images to Third Parties

7.6.1 Access to, and the disclosure of, images recorded by CCTV or other similar surveillance equipment must be strictly controlled by the System Manager. This is not only to protect the rights of the individual but also to ensure that the chain of evidence remains intact.

7.6.2 Access to recorded images must be restricted to those staff that need to have access in order to achieve the purpose(s) of using the equipment.

7.6.3 Disclosure of the recorded images to third parties (other than data subjects or managers within the Trust) can only be authorised by the Head of Service/ Nominated Deputy consultation with the Trust's Data Protection Officer.

7.6.4 Disclosure of recorded images to data subjects or managers within the Trust can be authorised by the System Manager or the Line Managers of the System Manager. Applications by managers within the Trust to System Managers for access or disclosure of recorded third party images must be approved by one of the following: Executive Director, Clinical or Service Director or Head of Service (see relevant forms at Appendices 1, 2 & 3). In all cases the reason(s) for disclosure must be compatible with the purpose(s) for which the images were originally obtained.

7.6.5 All requests for access or for disclosure to third parties must be documented. The reason(s) for disclosure must be compatible with the purpose(s) for which the images were originally obtained. Images must not be released to a third party without the consent of the data subject unless exception for the need to obtain the consent of the data subject is allowed within the Data Protection Act. For example, where disclosure is necessary for the prevention, or detection of any unlawful acts, where obtaining

consent would prejudice that purpose (e.g. passing information to the Police which may help them prevent a serious crime), If access or disclosure to images is denied, the reason must be documented.

7.6.6 If access or disclosure is allowed, then the following must be documented:

•The date of the application and, where appropriate, the date when the search fee was received.

•The date and time at which access was allowed or the date on which disclosure was made.

•The identification of any third party who was allowed access or to whom disclosure was made.

•The reason for allowing access or disclosure.

•The extent of the information to which access was allowed or which was disclosed. In certain circumstances it may be necessary for the images of some or all of the data subjects (together with any vehicle number plates) to be masked before access or disclosure is permitted – see Code of Practice.

7.7 Access by Data Subjects

7.7.1 The System Manager will be responsible for the production of an Information Sheet explaining the Trust's policy and procedures in relation to the CCTV Surveillance Installation which they manage. This leaflet must be given to any person making a request for access or disclosure of recorded images along with the Access Request Form (see Appendix 1). All requests from data subjects for access or disclosure of recorded images must be made using this form.

7.7.2 The Trust will only accept applications from the data subject, not persons acting on their behalf, except in cases where an application is made on behalf of a child under 16 years of age by someone with parental responsibility for the child or an application is made by a Legal Representative and the express consent of the data subject accompanies the request. Care must be taken when dealing with requests for recorded images of children from someone with parental responsibility for the child. Where children have the competence to understand the implications, and make an informed decision, about access to their recorded image, their consent must be sought rather than the person with parental responsibility.

7.7.3 As soon as the request is received the System Manager will arrange for the footage to be identified and preserved on suitable media. The System Manager will then send a written response to the data subject, after seeking advice from the Trust's Data Protection Officer, within one calendar month of receiving the request. This response will confirm whether there is a recorded image and the arrangements for access to view the recording. Access to recorded images must be facilitated within one calendar month of receiving a completed Access Request Form. If images of third parties are included in the images requested by the data subject, the System Manager must decide, taking advice from the Data Protection Officer whether the images of the third parties are held under a duty of confidence. If they are, the images of third parties must be masked before disclosure can be made. If,

exceptionally, images of third parties cannot be masked, access to the recorded material may be denied.

7.8 System Checks

7.8.1 System Managers must ensure that regular checks are carried out to ensure that the system is functioning satisfactorily and that the time recording function is accurate. Good practice would be to carry out daily checks of these functions.

7.8.2 Records must be kept of any checks carried out, when and by whom. Any identified faults should be reported as soon as practically possible through the Estates and Facilities Department.

8. DISPOSAL OF RECORDED IMAGES / DOCUMENTATION

8.1 All documentation relating to the management and operation of CCTV surveillance together with all Access Request Forms must be retained securely by the System Manager for a minimum of 3 years following which disposal may be authorised by the Head of the Service.

8.2 Any images that have been retained for evidential purposes will be retained for the minimum period necessary to serve that purpose which will necessarily need to be decided on a case by case basis

9. GUIDANCE ON THE USE OF CCTV DURING INTERNAL INVESTIGATIONS

9.1 CCTV is potentially an important part of evidence during an internal review or investigation as it can be used by the investigator(s) to assist in:

•Determining events including dates and times

•Identifying culprits, victims and witnesses

•Identifying inconsistencies in accounts

9.2 During the initial response to the report of an incident it is important that the responding manager (e.g. Duty Senior Nurse/ On Call Senior Manager) ensures that the CCTV footage is preserved and secured. In doing so, they should bear in mind that the CCTV footage that does not directly show the incident may be just as relevant as that which does. It is essential to therefore ensure that CCTV footage for adjoining areas is also retained together with the CCTV footage for the area of the incident not just for the period of the incident but also for a period pre and post the incident. If the incident has been reported to the police, advice must be sought from them via reporting staff as soon as possible about the CCTV footage to retain. If the police are investigating an incident, advice must be sought from the Head of service/

LSMS about the timing of any internal investigation and the management of evidence including CCTV.

NB It is important to note that CCTV is covered by the Data Protection Act when the information relates to a living individual who may be identified.

9.3 An investigator should be appointed as soon as possible and review the CCTV footage together with the other evidence. No one involved in the incident should be present when the investigator(s) view the CCTV material. This is especially important if those involved have not yet made a statement as it is necessary to avoid contamination of their memory. If it is necessary for the investigator(s) to view the CCTV with someone to identify images, it is important that this person is independent of the investigation. As part of the initial viewing of CCTV it is important to establish if the date and time displayed I s accurate.

9.4 If an investigator intends to introduce CCTV into an interview of someone involved in the incident, it should form part of the interview plan and structure. This will in turn determine the reasons why the footage is to be shown and at what point of the interview it should be presented e.g. the footage could be used to challenge an account if it differs from that portrayed in the CCTV. **The investigator(s) must be careful not to disclose anything that may influence the interviewee's recollection of events before a statement has been made.** A decision to disclose the CCTV by the investigator(s) must be made in the full knowledge of the likely consequences as it could affect the whole investigation as well as the interview and any subsequent hearing. If the investigator(s) are unsure about the disclosure of CCTV, the advice of the LSMS should be sought.

9.5 During the course of an investigation a request may be received from someone involved in an incident to view the CCTV. If so, the investigator needs to consider the impact this could have on the investigation. There is no requirement on investigators to disclose information including CCTV prior to an interview. It is for the investigator to decide. After completion of the investigation and prior to any hearing, arrangements may be made for relevant CCTV to be viewed by those involved together with their representatives. Any formal requests for copies of CCTV must be processed in accordance with this Policy.

9.6 Following the completion of any internal review or investigation, the CCTV footage should be retained with the investigation report and papers by the commissioning manager in accordance with record retention procedures.

10. COMPLAINTS PROCEDURE

10.1 Any complaints arising from the management and operation of CCTV surveillance will be dealt with under the Trust's normal complaints procedures as set out in complaints procedure. All complaints will be acknowledged in writing and the complainant will be advised that they may also refer the matter to the Information Commissioner if they are dissatisfied with the outcome of the Trust's investigation.

11. TRAINING

11.1 For each CCTV surveillance scheme, the Director/ Head of service with management responsibility for its operation will need to ensure that all relevant staff undergoes appropriate training in the operation of the CCTV system to include being made aware of the requirements of this policy, the Data Protection Act and the Code of Practice on the use of CCTV.

12. MONITORING/ REVIEW

12.1 It is the responsibility of the system managers to ensure that CCTV systems are installed and operated in compliance with this policy taking advice as appropriate from the Information Governance Manager and the Local Security Management Specialist.

12.2 Each system manager should carry out an annual review of the CCTV system against the operational policy to ensure that it is still achieving its original stated purpose. If it is not, then in liaison with the LSMS consideration should be given to discontinuing its use, or modifying the system to ensure it is compliant.

12.3 Any instances of non-compliance with the policy either at a systemic or individual level must be reported using the Trust's Incident Reporting procedures and dependant on the nature of the incident advice may need to be sought from the Information Governance Manager.

12.4 The Policy will be reviewed by the LSMS every 3 years or sooner where required.

13. REFERENCES/ SUPPORTING DOCUMENTS

- In the Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information' (2017)

- CCTV Operational Requirements Manual (2009) – Home Office Scientific Development Branch

- Data Protection Act (2018)

Appendix 1: FLOWCHART

CCTV is potentially an important part of evidence during an internal review or investigation as it can be used by the investigator(s) to assist in:

- determining events including dates and times
- identifying culprits, victims and witnesses
- identifying inconsistencies in accounts

⇩

During the initial response to the report of an incident, it is important that the responding manager (e.g. Site Manager/ Unit Coordinator/ Duty Senior Nurse/ On Call Senior Manager) ensures that the CCTV footage is preserved and secured. In doing so, they should bear in mind that the CCTV footage that does not directly show the incident may be just as relevant as that which does.

⇩

An investigator should be appointed as soon as possible and review the CCTV footage together with the other evidence. No one involved in the incident should be present when the investigator(s) view the CCTV material.

⇩

If an investigator intends to introduce CCTV into an interview of someone involved in the incident, it should form part of the interview plan and structure. This will in turn determine the reasons why the footage is to be shown and at what point of the interview it should be presented. **The investigator(s) must be careful not to disclose anything that may influence the interviewee's recollection of events before a statement has been made.**

⇩

During the course of an investigation a request may be received from someone involved in an incident to view the CCTV. If so, the investigator needs to consider the impact this could have on the investigation. There is no requirement on investigators to disclose information including CCTV prior to an interview. It is for the investigator to decide.

⇩

Following the completion of any internal review or investigation, the CCTV footage should be retained with the investigation report and papers by the commissioning manager in accordance with record retention procedures.

NB. This flowchart refers to the use of CCTV during internal investigations only

APPENDIX 2

APPLICATION FOR TRUST MANAGERS TO VIEW RECORDED IMAGES

Part A – Details of Application (to be completed by Applicant)
Please state the date, time and location of the images to be viewed: **Reason for request:** **Please provide the names of any others who will the viewing in addition to the applicant below:** **Name…… Signature……..** **Department ……. Date .....……** **Tel No…….....**
Part B – Approval (to be completed by the applicant's Head of Service/Associate Clinical Director)
Any additional comments in support of the request: Name …… Signature ..... Date ……

Part C – Authorisation by System Manager

Please state whether application is approved or whether any changes to the Applicant's request have been agreed. Also provide details of any images to be masked:

Name ……..……. Signature ……..…….

Date ……....

Part D – Record of Viewing (to be completed by the System Manager or designated staff)

Note date and time of viewing and persons present:

Name ……..…… Signature.....

Date……..

Appendix 3: APPLICATION FOR TRUST MANAGERS TO RECEIVE A COPY OF RECORDED IMAGES

Part A – Details of Application (to be completed by Applicant)

Please state the date, time and location of the images to be copied:

Reason for request:

Name……..Signature……

Department …….. Date……...

Tel No…….....

Part B – Approval (to be completed by the applicant's Head of Service/ Associate Clinical Directors)

Any additional comments in support of the request:

Name ……Signature ....

Date…….

Part C – Authorisation by System Manager

Please state whether application is approved or whether any changes to the Applicant's request have been agreed. Also provide details of any images to be masked:

Name ……..…… … … … Signature ..... ……...

Date……

Part D – Record of Copy (to be completed by the System Manager or designated person)

Note date and time that copy was produced and who by:

I confirm that I have checked the recording and it accords with the authorisation in Part C of this form.

Name ……..……. Signature.....……

Date……...

Part E – Receipt of Recording (to be completed by the Applicant)

I confirm receipt of the above and undertake to ensure that it is securely stored and returned to the System Manager for disposal.

Name …….. ……Signature ……. …..

Date ……..……....

Appendix 4 APPLICATION FOR ACCESS TO RECORDED IMAGES (subject access request)

The information requested below is to help East London Foundation NHS Trust to

a) Satisfy itself as to your identity and

b) Find any relevant data held

SECTION 1 ABOUT YOU								
Title (tick box)	Mr		Mrs		Miss		Ms	
Other title (e.g. Dr)								
Surname/family name								
First name(s)								
Maiden name / former name								
Sex (tick box)	Male				Female			
Height								
Date of Birth								
Place of Birth	Town				County			

Your current home address (to which we will reply)	
	Post code
A telephone number will be helpful in case we need to contact you	Tel No.

If you have lived at the above address for less than 10 years, please give your previous address(es) for this period

Previous Address(es)		
Dates of Occupancy	From	To
Dates of Occupancy	From	To

To help establish your identity, your application must be accompanied by copies of TWO official documents that, between them, show your name, date of birth and current address

For example, birth/adoption certificate, driving licence, medical card, passport or other official document that shows your name and address

Also TWO recent photographs of yourself, one of which if full face and the other a side perspective

Failure to provide this proof of identity may delay your application

SECTION 2	**PROOF OF IDENTITY**

DECLARATION (To be signed by the applicant)

……..

SECTION 3	**SUPPLY OF INFORMATION**

You have a right, subject to certain exceptions, to receive a copy of the information in a permanent form. Do you wish to:

a) view the information and receive a permanent copy?

b) only view the information?

Delete as appropriate

SECTION 4	**DECLARATION**

I have read and understood the accompanying information explaining East London Foundation NHS Trust's policy in relation to the purpose of the CCTV surveillance and the arrangements for access to recorded images.

I certify that the information that I have supplied in this application is true and accurate and that I am the person to whom it relates.

I understand that it is necessary for East London Foundation NHS Trust to confirm my identity and that it may be necessary to obtain more detailed information in order to locate the correct information.

Signed by		Date	
Please ensure that all Sections are completed <u>before</u> returning the form			
WARNING: A PERSON WHO IMPERSONATES OR ATTEMPTS TO IMPERSONATE ANOTHER, MAY BE GUILTY OF AN OFFENCE			

SECTION 5	**TO HELP US FIND THE INFORMATION**

Date(s) and time(s) of incident	
Place incident happened	
Vehicle Registration Number (if you believe that your image was captured whilst you were there travelling in your vehicle)	
Brief details of incident	

Use separate sheets if required

Before returning this form please check:	• Have you enclosed TWO identification documents? • Have you enclosed TWO recent photographs? • Have you signed and dated the form? •

NOTE: East London Foundation NHS Trust reserves the right to obscure or suppress information relating to other third parties (under the terms of the Data Protection Act 2018)

SIGNED		DATE	

A written response to your application will be made within one calendar month

Further information and advice may be obtained from:

http://www.ico.org.uk/