CLOSED CIRCUIT TELEVISION (CCTV) PROCEDURE

PROCEDURE SUMMARY
The purpose of this Procedure is to ensure employees of Essex Partnership University NHS Foundation Trust are provided with clear guidance on the regulation, management and use of Closed Circuit Television (CCTV) systems throughout its premises and is be read in conjunction with the CP28 Closed Circuit Television (CCTV) Policy.

The Trust monitors the implementation of and compliance with this procedure in the following ways;

The Director responsible for monitoring and reviewing this Procedure is the Executive Chief Finance & Resources Officer.
CONTENTS

THIS IS AN INTERACTIVE CONTENTS PAGE, BY CLICKING ON THE TITLES BELOW YOU WILL BE TAKEN TO THE SECTION THAT YOU WANT.

1.0 INTRODUCTION

2.0 ASSESSMENT PROCESS FOR INSTALLATIONS OF CCTV SYSTEMS

3.0 USE OF CCTV IN MENTAL HEALTH SETTINGS

4.0 DATA PROTECTION LEGISLATION

5.0 MANAGEMENT OF ALL CCTV SCHEMES

6.0 TRAINING

7.0 DISCLOSURE

8.0 SUBJECT ACCESS REQUESTS

9.0 DESTRUCTION OF DATA

10.0 PHYSICAL SECURITY ADVISOR

APPENDICES

APPENDIX 1 – SUBJECT ACCESS REQUEST FORM

APPENDIX 2 – POLICE - REQUEST TO ACCESS FORM
1.0 INTRODUCTION

1.1 This procedure guidance sets out the responsibilities and processes to be followed in relation to the assessment, installation, maintenance and management of the Closed Circuit Television (CCTV) surveillance systems at Essex Partnership University NHS Foundation Trust sites and at sites where Trust staff reside.

1.2 This document has been written in accordance with and adheres to the principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018, Human Rights Act (1998) and the CCTV Code of Practice (2016) and guidance issued in the NHS Security Manual (chapter 5 Closed Circuit Television (CCTV)).

1.3 The purpose of this Guidance is to ensure that:
- Any CCTV systems are justified, appropriately managed and not open to abuse or misuse.
- Correct assessments are made in relation to the need for any CCTV scheme
- Standards are applied to ensure schemes are valid.
- CCTV is appropriately installed, maintained and managed.
- Responsibility for the management of CCTV systems is identified at both local and Trust wide level.
- Access, storage and disclosure of images are in accordance with the principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018 and with Trust policy on data protection.
- The identification and training of data managers for each location where the Trust is the Data Controller of a CCTV system

2.0 ASSESSMENT PROCESS FOR THE INSTALLATIONS OF CCTV SYSTEMS

2.1 Where consideration is being given to the installation of a new or replacement CCTV system this will be co-ordinated and led by the Trust Physical Security Advisor (PSA). No installation, maintenance or alteration will take place without the explicit agreement of this individual who has knowledge and expertise in the use and management of CCTV and will advise operational managers on the Procurement, use and management of CCTV systems.

2.2 The PSA will carry out a Data Privacy Impact Assessment to establish the justification and requirement for the installation of CCTV.

2.3 The PSA and or LSMS will consider all possible options in relation to any request for CCTV and whether other cost effective solutions are available, including less intrusive means of achieving the same objective. Where a CCTV system is considered to be the most suitable solution to meet the requirement this should be documented.

2.4 The survey should identify those who need to view live footage and those needing to review recorded footage and the systems made available to fulfil this need. Those offering a monitoring service to a live feed from a high risk environment e.g. Seclusion room should have a monitor for each camera view to reduce the time taken to switch between images unless that switch is immediate. To protect the
integrity of IT Comms Rooms the use of remote access on site allows users to access recorded footage from their PC terminal.

2.5 In line with the CCTV Policy all installations must offer evidence-quality footage therefore when undertaking repairs, replacing or installing parts or complete systems, efficient access to data and value for money must be considered alongside achieving enhancements to meet ICO guidance where possible.

2.6 CCTV installations should be supported with regards sufficient lighting as well as cameras not being impeded in view by overgrown bushes or other obstructions.

2.7 CCTV systems should record continuously and not restricted to movement activated. Although movement activated can benefit the memory capabilities of the hardware, the captured footage is often short by a few seconds missing vital elements of the incident. There are also many investigations where no movement is beneficial evidence i.e. if tracking a missing person to show they did not go that route.

2.8 CCTV recording in inpatient communal areas has been previously assessed, offering a valuable solution to the ability to obtain evidence following many types of incident not limited to criminal damage, violence and aggression and injuries from slips, trips or falls affecting the Trust its service users, visitors or staff. The ability to offer a tool for ward de-briefs and management feedback is also invaluable for the development of a safer environment. The above installations however, require regular review and local assessment; usually highlighting a need for an increase in signage for those who may not have entered the site via the front door. E.g. 136 or where capacity fluctuates.

2.9 When a decision is made to install CCTV into communal patient areas, and whenever new patients enter the ward, patients should be advised of the system and the reasons for its use. Whilst patients consent to its use is preferable, it is not required when the purpose of the system is believed to be in the best interests of the patient or others on the ward,

2.10 In addition, within the design phase, it is the PSA role to liaise with other stakeholders of the scheme to support the installation:
- ITT/CSU for connection to the Trust Network – this would require being allocated an IP Address, port access, rack space and UPS resilience.
- Liaise with Area Maintenance teams to detail the approved maintenance schedule of the system
- Discuss and agree how repairs will be effected when identified (including response times)
- Consultation with the IG Team/Data Protection Officer

2.11 The installation of CCTV systems and maintenance schedules will only be carried out by companies that are approved by the Trust and comply with UK Regulatory bodies a such as National Security Inspectorate (NSI) and the Security Systems and Alarms Inspectorate Board (SSAIB).

2.12 In addition to national requirements, the Trust requires identified installers and maintainers to comply with the Trust Policy for Contractors adhering to individual sites security protocols and Trust information sharing agreements
2.13 Once installed the extent to which the requirement of the system has been fulfilled will be assessed. During installation the PSA and or LSMS may make arrangements to modify the system until it meets the defined requirement.

### 3.0 USE OF CCTV IN MENTAL HEALTH SETTINGS

3.1 CCTV cannot and is not designed to replace clinical care or as a means to answer security concerns. It does not and cannot replace skilled employees as a method of observing patient behaviour.

3.2 There are three types of “psychiatric unit area” that is defined for CCTV coverage.

- Public areas
- Communal areas
- Private area

3.3 **Public areas**: These are areas to which the public have unrestricted access: grounds, corridors, car parks etc.

3.4 **Communal areas**: Parts of wards shared by all patients; day rooms, dinning areas, corridors etc.

3.5 There are no special considerations required for Public or Communal areas beyond those required by the Information Commissioner on all CCTV cameras, such as signage, registration etc., and that a clear reason for installation is available. This policy covers those requirements.

3.6 **Private areas**: these are areas where any individual might reasonably expect privacy. These include bathrooms, bedrooms, toilets and seclusion rooms.

3.7 The use of monitoring CCTV (not recordable) within private areas is only routinely authorised for Seclusion Rooms and 136 environments. In the event further is considered or the desire for recordable in these areas considered it will need to be justified by appropriate clinical directors/managers.

3.8 Prior to consideration of approval for the use of CCTV within a private area, appropriate local policies, procedures and protocols will need to be in place and all clinical staff need to be fully conversant and able to demonstrate knowledge of appropriate polices, procedures and local protocols.

3.9 Any authorisation that is granted for the use of CCTV within any private area will be subject to regular review and monitoring by the Trust LSMS and or PSA.

### 4.0 DATA PROTECTION LEGISLATION

4.1 The Trust will identify, list and document all its CCTV schemes within the “Notification” ('registration of data systems'), which it is required to make to the Information Commissioner under the terms of the General Data Protection Regulation 2016 and the Data Protection Act 2018.
4.2 To comply with the current Data Protection Act legislation, all operational management of the Trust CCTV schemes will conform to guidance within “Information Commissioner CCTV Code of Practice” published by the Information Commissioner (a copy of which is available from the Information Governance Manager). In order to conform to this code of practice the following guidelines must be adhered to:

- The local data manager responsible for the CCTV system at their premises will be responsible for managing the system and for maintaining compliance with relevant polices and procedures. The data manager will also be responsible for the management and control of all imagery that is downloaded locally in accordance with this policy including appropriate, back-up, retention, and destruction of all storage media and that it is conducted in accordance with the written operational procedures.

- Cameras will not be hidden from view and appropriate steps must be taken, e.g. by signing and display posters, to inform employees, patients, visitors and the public of the presence of the CCTV surveillance system in use, its purpose and the Trust name and contact details, including a working telephone number, of who can provide further information if requested. To ensure privacy the cameras are fixed and focussed to observe Trust property, which can be demonstrated upon receiving a specific request.

- Images from the cameras are appropriately recorded, maintained and managed in accordance with these operational procedures and wider Policy.

- There is no audio recording undertaken from any part of the Trust CCTV systems.

4.3 In order to comply with the General Data Protection Regulation 2016 and the Data Protection Act 2018, the following standards must be met:

- All imagery must be fairly and lawfully processed;
- All imagery will only be maintained for specific purposes All CCTV installations will be proportionate and not excessive;
- All contractors with the capability of accessing CCTV data whether via periodic maintenance contracts or one-off tasks generated to undertake a download of footage regarding an incident must hold an information sharing agreement with the Trust.
- All CCTV imagery will be processed in accordance with individuals rights;
- CCTV imagery will not be transferred to countries outside of the EEA without adequate protection.

5.0 MANAGEMENT OF ALL CCTV SCHEMES

5.1 Operational and day to day management of all Trust CCTV schemes will be the responsibility of the PSA. Delegated responsibility will be to local departmental/unit Data Managers and appropriate nominated personnel.
5.2 Specific duties may include but are not restricted to:

- Records of Maintenance of CCTV
- Information to include
  - Location
  - Buildings
  - Number of cameras and type
  - Local data manager
  - 3rd party maintenance contractor.
  - Date last maintained.

- Coordination of CCTV training via a third party supplier (see section 6.0).
- Production of CCTV reports and assessments of current and or proposed schemes.
- Auditing and monitoring of CCTV schemes.
- Ensuring all CCTV systems are installed appropriately and meets the defined requirements.
- Coordinating the downloading of imagery where required under section 7.0.
- Ensure that no image is stored for any longer than necessary. Except where held for specific circumstances, legal proceedings, criminal investigation, prosecution or for evaluating incident statistics, patterns or behaviours etc.

5.3 Day to day Operational Duties are the responsibility of the local staff overseen by Team Management where the CCTV system resides – duties are:

- To ensure daily the time and date are accurate
- To immediately report any failures in equipment (cameras or hardware)
- To ensure a trained person, in the playback of footage, is available in the event of an incident
- To highlight any deficiencies in coverage that exposes the site or staff to an increase in risk in the event the service or layout changes.
- To report via Datix any need for accessing the system and when an incident occurs requiring footage to be captured that the PSA (Physical Security Advisor) is contacted as soon as possible to secure footage.
- To ensure as part of local induction that staff are aware who to escalate access to footage queries to and the requirement for the completion of the access to footage form (see Appendix)
- To ensure the PSA is included in any discussions where the coverage of CCTV could be affected i.e. due to the change of use of an area

5.4 Whilst a retention period of 31 days is often quoted, retention periods are not mandated in law. The legal definition is for as long as necessary for the purpose. The Trust’s portfolio of CCTV is diverse and retention periods vary from site to site, in some cases dependent upon the capacity of the technology. However the Trust attempts to fulfil a minimum of 31 days unless specifically stated.

6.0 TRAINING

6.1 Training to a basic user level is initially available from the contractor during installation but once the training has been provided it will be the responsibility of the unit/facility manager to ensure they maintain an appropriate number of trained employees via liaison with the PSA and appropriate records are maintained,
including the date and type of training received and date of any planned refresher training as required.

6.2 Reviewing CCTV for the purposes of identifying the direction of travel of an absconder or providing an accurate description to Police to assist a search or identify an assailant can be efficiently undertaken via desktop terminals for systems that are on the Trust IT network. Others require manual operation of the DVR unit itself which may require access to offices, Comms rooms or other restricted access locations. It is the Unit Managers responsibility to ensure those requiring access in/out of hours have the ability to gain access when authorised.

6.3 CCTV training will include
   1. Basic user training
   2. Record keeping
   3. Data protection and CCTV code of practice
   4. Reporting procedures
   5. Basic fault finding and maintenance call out procedures
   6. Imagery download procedures and evidence handling

6.4 Refresher or additional staff training can be requested via the PSA. This training would often be outsourced to the maintenance contractor and cross charged.

6.5 Local access for users provides a restricted level so as not allow formatting of hard drives or altering of camera capabilities and quality.

7.0 DISCLOSURE OF FOOTAGE

7.1 Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it may be appropriate to disclose images to law enforcement agencies where a crime needs to be investigated. Even if a system was not established to prevent and detect crime, it may still be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

7.2 Any other requests for images should be approached with care, as a wide disclosure of these may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where their needs outweigh those of the individuals whose images are recorded.

7.3 Failure to protect the data of subjects or the integrity of the system would likely result in disciplinary procedures being brought against not only the individual(s) undertaking the access but also those sharing it.

7.4 The PSA has access to the networked CCTV systems and can download, review and share required footage internally via secure options, i.e. file transfer.

7.5 Where CCTV systems are not networked it will require liaison with locally competent staff or dedicated contractor to access footage. This will then be reviewed by the PSA before disseminating, if required.
7.6 When providing footage as evidence to law enforcement agencies, following a subject access request form being completed and authorised, the limited footage is copied to an encrypted memory stick or DVD, placed in an evidence bag and where required a statement taken by Officers relating to the capture. Officers rarely get to see the image from the disc or media device for many weeks as this media will not playback on their computers and requires their own internal processes of upload and decryption to occur. Thus on most occasions the investigating officer will require viewing the footage at Trust premises to allow their case to progress in a timely manner. The footage then becomes an exhibit in the investigation.

7.7 The person capturing/securing/seizing the footage may be required as a witness to the case and by undertaking the task trained staff accept the duties and responsibilities of this. Where possible the preference is for the PSA to undertake this, failing this to provide support to those staff that enter into this position.

7.8 Requests for access to footage should have an associated Datix. Whether a missing person (misper), car damage or assault, an incident must be reported in line with the Trust incident reporting guidelines. This does not require an additional Datix if it relates to an existing incident; however, in the event Police request footage of a non-Trust related incident a Datix would then be raised. Exclusions to this would be HR investigations or those where completing a Datix could jeopardise the confidentiality of the incident.

8.0 SUBJECT ACCESS REQUESTS

8.1 Where specific formal requests by individuals who are “data subjects” are made this will be managed by the Trust’s Data Protection Officer in liaison with the PSA and Legal Team. They will permit subject access to the images recorded by the system according to the processes set out in the Trust’s Information Governance procedural guidance and CCTV code of practice.

8.2 Disclosure of images to third parties should only be made in limited and prescribed circumstances. For example the prevention and detection of crime where disclosure to a third party (Police) would assist in a specific criminal enquiry, security issues or in pursuit of criminal activity or requested by the Police this will be managed by the Legal Team in liaison with the PSA. Where this type of request is made the form “Request from Police to access and obtain / receive copies of closed circuit television CCTV media” Appendix 2 will be completed and sent to the Trust’s Legal Team.

8.3 If the data subject does not know the date and approximate time of the material being sought, the Trust will not proceed to conduct lengthy searches of the correct images of the data subject.

8.4 The Trust’s Legal Team will have responsibility to determine whether to comply with a request for access to CCTV images and to determine whether disclosure of images would entail disclosing images of third parties. If a third party identity cannot be removed then the request may be denied. Where access is denied the individual will receive a written response stating why within 1 (one) calendar month of receiving the completed “Subject Access request form".
8.5 Where media is or may be required for evidential purposes in legal proceedings, or requested by legal representatives (solicitors, Crown Prosecution Service etc.), it will be kept and stored under designated secure environments until all legal proceedings are exhausted. This will usually be undertaken by the PSA utilising central Trust secure servers or secured locally in hard format in a locked, controlled facility.

8.6 Any member of staff receiving such a request should forward it immediately to the Trust’s Legal Team, ensuring that the PSA is copied in on all email correspondence.

9.0 DESTRUCTION OF DATA

9.1 Advice must be obtained for each individual case, however, options exist for the destruction of data that include the use of clinical waste services, shredding and handing it over to the PSA to undertake.

9.2 Format-able data media i.e. memory sticks, hard drives and rewritable discs are not considered destroyed simply by formatting/deleting due to software being available that allows the ability to reconstruct the data previously stored on such devices.

10.0 PHYSICAL SECURITY ADVISOR - PSA

10.1 The PSA offers the advice and recommendation regarding specification and suitability of installation along with expert technical awareness of CCTV hardware and software for interrogation of faults/failures and a multi facet of software platforms for capturing data for investigation.

10.2 Timescales of investigation can vary based on priority and the system accessibility however, all appropriate parties will be kept informed of the stages during each request.

- Identify camera locations – would the apparent incident have been captured?
- Identify timings – system calibrated correctly, vague timings? “Review full shift”
- Is the Trust the Data Controller – where not, liaise with landlord
- Is somebody suitably trained locally? – consider use of contractor if more efficient and incident requires urgent response.
- Where systems are remotely accessible it is often more efficient to download the data prior to review to allow for 16x fast forward capability compared to remote limitations in connectivity.
- Various camera images can be edited together to provide a sequence of events, where possible.
- Editing software can be utilised to blur faces/number plates where required.

10.3 There will be incidents or circumstances where Management are required to review the actions of staff during an incident or leading up to, this CCTV may be shared remotely with the use of Trust servers for local review by the Manager. The
same restrictions apply and these are not to be shared, copied or abused to prevent harm to the subjects captured within the footage.

10.4 PSA to liaise with Maintenance management regarding remedial works to ensure these support longer term strategy of installations.
Access to CCTV images required (Request should be within 21 days of incident)

**URGENT ACCESS:**
Missing Person/Absconds

Identified persons at site hold access codes for reviewing footage to ascertain time critical information e.g. clothes worn or direction of travel

Incident must be Datix’d referencing if access to CCTV occurs and PSA liaison

**Internal staff investigation**
(HR/Management)

Liaise directly with PSA

**Alleged Incident**
i.e. potential damage to car in car park

**Contact PSA to assist with obtaining footage**

If footage is required to be shared further – Contact PSA & Legal Team i.e. Police social media campaign

**Non-Staff Request**
(Police / Insurers / 3rd Parties)
To view or obtain copies of images/footage

**Complete formal request. Appendix 1 or 2.**
Subject Access Request or Police Release Form

Request sent to Legal Team to process

Images provided by PSA to Legal

Appropriate release or refusal of request facilitated by Legal Team

END