CLOSED CIRCUIT TELEVISION (CCTV) POLICY

<table>
<thead>
<tr>
<th>POLICY REFERENCE NUMBER:</th>
<th>CP28</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERSION NUMBER:</td>
<td>3</td>
</tr>
<tr>
<td>REPLACES SEPT DOCUMENT</td>
<td>CP28 v2</td>
</tr>
<tr>
<td>REPLACES NEP DOCUMENT</td>
<td>CP4/CCTV/03/13</td>
</tr>
<tr>
<td>KEY CHANGES FROM PREVIOUS VERSION</td>
<td></td>
</tr>
<tr>
<td>AUTHOR:</td>
<td>Physical Security Advisor</td>
</tr>
<tr>
<td>CONSULTATION GROUPS:</td>
<td>HSSC</td>
</tr>
<tr>
<td>IMPLEMENTATION DATE:</td>
<td>1st June 2018</td>
</tr>
<tr>
<td>AMENDMENT DATE(S):</td>
<td>NA</td>
</tr>
<tr>
<td>LAST REVIEW DATE:</td>
<td>September 2014, April 18</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>April 2021</td>
</tr>
<tr>
<td>APPROVAL BY HEALTH, SAFETY &amp; SECURITY COMMITTEE:</td>
<td>21st May 2018</td>
</tr>
<tr>
<td>RATIFICATION BY QUALITY COMMITTEE:</td>
<td>Chair’s Action June 18</td>
</tr>
<tr>
<td>COPYRIGHT:</td>
<td>2018</td>
</tr>
</tbody>
</table>

POLICY SUMMARY

The purpose of this policy 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 CPG28 Closed Circuit Television (CCTV) Procedure.

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

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>APPLICABLE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRUSTWIDE</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

THE DIRECTOR RESPONSIBLE FOR MONITORING AND REVIEWING THIS POLICY IS EXECUTIVE CHIEF FINANCE & RESOURCES OFFICER
ESSEX PARTNERSHIP UNIVERSITY NHS FOUNDATION TRUST

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 SCOPE
3.0 DEFINITIONS
4.0 RESPONSIBILITIES
5.0 OWNERSHIP AND OPERATION OF CCTV SCHEMES
6.0 PRINCIPLES
7.0 PURPOSE OF CCTV SCHEMES
8.0 BREACHES OF THIS POLICY
9.0 COMPLAINTS PROCEDURE
10.0 IMPLEMENTATION OF POLICY
11.0 REFERENCES
12.0 REVIEW OF THIS POLICY
1.0 INTRODUCTION

1.1 This policy and associated procedural guidance sets out the responsibilities and processes to be followed in relation to the request, installation, management and upgrading of the Closed Circuit Television (CCTV) surveillance systems on Essex Partnership University NHS Foundation Trust sites.

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 policy is to ensure that:
- Any CCTV systems are justified, appropriately managed and not open to abuse or misuse.
- Correct data privacy impact assessments are made in relation to the need for any CCTV system.
- 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 sharing.
- Sites have immediate access to recorded footage requiring training to have occurred to an appropriate level.

2.0 SCOPE

2.1 This policy and its procedural guidance is binding on all employees of the Trust and applies also to other persons who may, from time to time, and for whatever purpose, be present on Trust premises.

2.2 It is also intended to cover service areas of the Trust where activities are carried out, including those properties not owned but used by the Trust.

2.3 Any CCTV internal or removable drives, including CD’s, DVD’s, Memory sticks or hard drives are also deemed to be part of the CCTV system and will therefore be covered by the content of this policy.

2.4 This policy refers only to overt CCTV surveillance.

2.5 “Covert Surveillance” is where CCTV may be hidden or placed discreetly and may be used in sensitive investigations where on going problems occur within specific areas. The Trust does not have the authority to authorise the use of this type of surveillance. If it is thought that covert CCTV is required the PSA and or LSMS must be consulted who will seek guidance from the Police on an
appropriate course of action. Covert surveillance is not permitted within the Trust without legal RIPA (Regulation of Investigating Powers Act 2000) authorisation from the Police and the consent of the Trust Chief Executive.

3.0 DEFINITIONS

3.1 The following definitions will apply to this policy:

- The “Trust”- Essex Partnership University NHS Foundation Trust.
- CCTV-Closed Circuit television (CCTV) is the use of video cameras to transmit a signal to a specific set of monitors.
- ‘Scheme/System’- Any of the Trust’s CCTV schemes (a systematic plan for a course of action)
- LSMS – Accredited Local Security Management Specialist with generic knowledge of CCTV procedures.
- PSA -Physical Security Advisor who has managerial responsibility for all Trust CCTV systems and extensive knowledge of installations and functionality.
- Data Protection Officer - The Trust Legal Services Manager
- CCTV Minimum Specification – The minimum system standard that the Trust will authorise for installation and use
- Data Controller – Decides what is to be recorded, how the information should be used and to whom it may be disclosed.
- Data Manager - Individual with responsibility for localised CCTV system management i.e. Access to reviewing of, efficient reporting of failure/outages, informing Data Controller of site changes affecting CCTV.

3.2 The systems may capture images of where individuals (subjects) or their vehicle registrations can be identified. Under the General Data Protection Regulation 2016 this is deemed personal data.

4.0 RESPONSIBILITIES

4.1 The Trust Board of Directors has overall responsibility for ensuring the principles of this policy and procedures and other associated policies are implemented across the organisation. The duty of ensuring all measures needed to implement the CCTV policy and associated procedural guidelines is delegated to Directors within their areas of responsibility.

4.2 The Trust Board of Directors is fully committed to a culture of providing high quality healthcare and improving patient safety, this embraces the implementation of the principles of this policy which will be monitored through Clinical and Risk Management Governance.

4.3 The Director of ITT will ensure:

- Network availability for the use of CCTV across the Trust
- Where possible to accommodate CCTV DVR storage systems within Comms cabinets utilising the UPS.
• The provision and support of obtaining IP address details (subnet mask/Default gateway) to enable CCTV systems to be connected to the Trust network
• That the PSA is included in discussions relating to reconfigurations of Comms rooms at sites where CCTV is in operation to allow for safer storage and resilience of hardware.

4.4 Directors and Senior Management will have responsibility within their own service area for;

• Monitoring the implementation of this policy via audit and supervision.
• Ensuring staff receive effective training and that they are competent to implement the principles of this policy
• Ensure training records are maintained
• Be able to evidence that EPUT policies have been followed during any level of investigation.

4.5 Capital development and all site refurbishment project design must incorporate the appropriateness of CCTV installation by involving the PSA at the earliest stage. Latest technology and precedence of installation must be considered.

4.6 PSA and LSMS have designated responsibilities in the assessment of any CCTV scheme implemented and on-going responsibilities in relation to the operation and management of any scheme. These are detailed in the procedural guidance. This is to include the completion of a data privacy impact assessment (DPIA); an evaluation of proportionality and necessity. DPIA’s must be reviewed by the Information Governance team and the views and advice of the Data Protection Officer sought.

4.7 The PSA is identified as the data manager with authority for the following:
• Security and storage of data
• Security clearance of persons (staff & contractors) who have experience/competence to use the system appropriately for immediate review to assist locate absconder or other time sensitive footage
• Release of new, and destruction of old data and data media specifically relating to the internal hard drives contained within the CCTV hardware.
• Overarching design and control of installations and directing competent contractors to provide maintenance and remedial actions
• Liaison with ITT & CSU to resolve conversion and codec issues with playback of recorded footage for investigation.
• Liaison with the law enforcement agencies and other requesting parties; relating to installations, coverage and potential/likelihood of capturing requested incident
• In conjunction with respective Information Governance or Legal team, responsible for identifying non-compliance with the British Standard and/or legislation, operational procedures and breaches of confidentiality including unauthorised sharing of data.
4.8 Where CCTV impacts on service users, staff and members of the public Data Managers and or other Persons in Charge / Team Leaders / Ward Managers and Senior Sisters, where identified as the nominated contact point, will:

- Ensure the procedures and principles detailed within this policy and associated procedural guidance are followed and monitored to meet all relevant guidance.

4.9 Individuals working with or utilising any CCTV system have a responsibility to ensure that the principles contained within this policy and associated guidelines are followed; in that they:

- Have an understanding of the CCTV policy, procedures and local protocols.
- Implement those areas of this policy and procedural guidance that falls within their work remit.
- Identify any use of CCTV that may result in a breach of this policy.

4.10 All staff utilising CCTV, whether live monitoring or playback must ensure that all outages, reduction in quality or time calibration matters are immediately escalated to the Estates & Facilities department for further investigation / resolution.

5.0 OWNERSHIP AND OPERATION OF CCTV SCHEMES

5.1 The majority of CCTV schemes are owned and operated by the Trust. Therefore cameras, monitors, data collection and retention processes are managed maintained operationally by designated staff, Data managers, on each respective Trust site and further maintained by approved 3rd party provider organisations under a separate maintenance contract to the Trust in accordance with this policy.

5.2 Properties do exist where the Trust occupation is under a lease arrangement and the CCTV system may be owned or controlled by a landlord. The access of and compliance with statutory duties is their responsibility and the Trust is required to ensure information sharing agreements are in place to enable efficient access to data and reassurance regarding compliance with their statutory duties. If the system owner has not taken steps to inform visitors that the system is in place we retain a duty to inform our visitors and staff that CCTV is in place even if we do not have knowledge of the extent of its capability's or coverage.

5.3 Responsibility for the review, assessment, installation, and maintenance of all CCTV systems, data collection and control of images and the training of staff is delegated to the Physical Security Advisor.

5.4 All CCTV systems must offer the capability for efficient reviewing of footage to support incident investigation or obtain time sensitive detail i.e. Absconder direction of travel or identifying clothes worn. Therefore all Trust owned
systems must be attached to the Trust IT network for remote access by the PSA or other trained persons.

5.5 To support the retention of valuable data and the ability to provide observation of high risk environments, the recordable CCTV systems must be attached to a UPS (uninterrupted power supply) whether by a standalone unit or as part of a sites IT infrastructure.

5.6 Signage must be displayed on all sites with recordable CCTV systems. The standardised signage identifying the contact point to request access to footage and the reasons for installation must be located on the approach to enter a building (potentially multiple access points). It is also good practice to repeat CCTV signage or increase awareness within a site where those who frequent may not have held capacity when initially entering the site e.g. via s.136 or when CCTV exists within a ward environment where capacity may fluctuate.

6.0 PRINCIPLES

6.1 The following principles govern the operation of all schemes:
CCTV is used for maintaining the security of property and premises and for preventing and investigating crime, it may also be used to monitor staff when carrying out work duties. For these reasons the information processed may include visual images, personal appearance and behaviours. This information may be about staff, customers and clients, offenders and suspected offenders, members of the public and those inside, entering or in the immediate vicinity of the area under surveillance. Where necessary or required this information is shared with the data subjects themselves, employees and agents, services providers, police forces, security organisations and persons making an enquiry.

6.2 Data Protection issues:

- All schemes will be operated fairly and lawfully in accordance with the principles of the General Data Protection Regulation 2016 and the Data Protection Act 2018; Human Rights Act (1998) and only for the defined purpose set out in Section 6 and in accordance with Section 10 of this guidance. (See also section 7.0 below).
- All schemes will be operated with due consideration for the privacy of individuals
- All Trust CCTV systems are to be registered with the Information Governance Manager
- Any change to the purpose for which any scheme is operated (Section 6) will require the prior approval of the PSA and consultation with the Trust’s Data Protection Officer and Information Governance team.
6.3 General management:

- All schemes will be monitored and managed in accordance with this policy and must be formally approved following a data privacy impact assessment prior to any installation.
- Prior to installation the PSA and or LSMS in conjunction with relevant services managers will carry out assessments to establish and determine the CCTV requirements and impact.
- Day to day compliance of CCTV systems operational management will be documented by the Data Manager and or authorised personnel and audited by the PSA.
- All CCTV installations must be of a minimum in quality that supports the purpose(s) for which they are intended i.e. Evidential quality for identification of an assailant/vehicle for the Criminal Justice system.
- Faults, outages and time calibration that affect the quality of capture must be reported to the Estates & Facilities team immediately.

6.4 Effective administration of installations should exist. To include locations of cameras and hardware along with installation date, projected lifespan of internal hard drives and basic system specification.

### 7.0 PURPOSE OF CCTV SCHEMES

7.1 The overall purpose of CCTV schemes is to support the health and safety of all persons on Trust properties to identify, manage and reduce risks and to help reduce the fear of crime for Trust staff and the general public; and to protect Trust premises from criminal activity.

7.2 CCTV cannot replace clinical care and is by no means the answer to all security concerns, it does, nonetheless, offer a potential medium by which personnel can enhance levels of care and security.

7.3 CCTV should not be wholly relied upon to provide all evidence to incidents, no audio is captured via CCTV and therefore witness statements are fundamental to reduce circumstantial accusations and support the facts of the case.

7.4 The particular purpose of all schemes unless specifically identified as directed monitoring (Section 8 in procedural guidance refers) is:

- To assist in the prevention and detection of crime against both persons and property.
- To provide a deterrent effect and reduce criminal activity.
- To offer identification for access into premises.
- To help identify, apprehend and prosecute offenders in relation to crime.
- Assist with absconson incidents, identifying direction of travel, clothing worn etc.
CP28 - CLOSED CIRCUIT TELEVISION (CCTV) Policy

- To protect and ensure the security of property and assets belonging to the Trust, its employees and visitors to Trust sites.
- To support the Police, PSA and LSMS in deterring and detecting anti-social behaviour.
- Assists with the safety of service users when in seclusion rooms, by providing extra observation tools (these images are not recorded)
- Where appropriate to assist in the circumstances where internal disciplinary procedures are required.
- To increase personal safety and reduce the fear of crime.

8.0 BREACHES OF THIS POLICY

8.1 The Trust reserves the right to take appropriate disciplinary action against any employee who breaches this policy in accordance with the Trust’s disciplinary procedures.

8.2 As a major purpose of these schemes is in assisting to safeguard the health and safety of staff, patients, and visitors (Section 6 refers), it should be noted that intentional or reckless interference with any part of any monitoring equipment, including cameras/monitors/or any associated multimedia equipment or device, including ancillary items, may be a criminal offence and will be regarded as a serious breach of Trust policy and subject to possible disciplinary procedures.

9.0 COMPLAINTS PROCEDURE

9.1 Data subjects who feel they may have grievances and complaints concerning the operation of the Trust’s closed circuit television scheme may progress through the Information Governance Team or the Data Protection Officer Details of which should be available from any trust location or via a telephone information line.

9.2 Alternatively, if the data subject is not satisfied with the response, he/she may contact the Information Commissioner. The Crown appoints the Commissioner and their main function is to enforce compliance under the legislation.

10.0 IMPLEMENTATION OF POLICY

10.1. This policy will be disseminated across the organisation through the Trust Intranet site.
11.0 REFERENCES

11.1 Other related policies include:

- Data Protection & Confidentiality Policy / Procedures
- Security Policy
- Prevention and Management of Violence and Aggression
- In-patient Observation Policy
- Missing Patient Policy
- Freedom of Information Policy / Procedures
- Information Governance & Security Policy / Procedures
- Information Sharing & Consent Policy / Procedures

(This list is not exhaustive)

11.2 Related Legislation and Publications:

- General Data Protection Regulation 2016 and the Data Protection Act 2018
- The CCTV Code of Practice produced by the Information Commissioner
- The CCTV Code of Practice revised edition 2016
- The Human Rights Act 1998
- Caldecott Report 1997
- Health and Safety at Work Act 1974

(This list is not exhaustive)

12.0 REVIEW OF THIS POLICY

12.1 This policy, its implementation and the operation of the Trust’s CCTV schemes, will be reviewed by the PSA and or LSMS in conjunction with the Information Governance Manager, every three years or as required during that period before review.

END