Lincolnshire Community Health Services
NHS Trust

CCTV POLICY
(LCHS OWNED SITES)

Reference No:	P_HS_13
Version:	4.1
Ratified by:	LCHS Trust Board
Date ratified:	14 August 2018
Name of originator/author:	Local Security Management Specialist Head of Estates and Facilities Management
Name of responsible committee/individual:	Health & Safety Committee
Date issued:	August 2018
Review date:	December 2021
Target audience:	All Staff
Distributed via:	Website

Lincolnshire Community Health Services NHS Trust

CCTV Policy (LCHS Owned Sites)

Version Control Sheet

Version	Section/Para/ Appendix	Version/Description of Amendments	Date	Author/Amended by
1		NHSL Policy Adopted	March 10	
2		Full review and update – new reference (old HS001)	July 2014	Travers Ramsden
3		Full review	May 2016	Carl Kisby
4		Update to new trust branding, general Review	May 2018	Carl Kisby, Craig Evans
4.1	Entire document	This document has been checked by the policy owner who has confirmed that it is fit for use and that it will be fully reviewed and updated as appropriate before the end of the extension period granted by LCHS Trust Board on 12/1/2021	January 2021	Corporate Governance Team
5				
6				
7				

Lincolnshire Community Health Services NHS Trust

CCTV Policy (LCHS Owned Sites)

Contents

Lincolnshire Community Health Services NHS Trust

CCTV Policy (LCHS Owned Sites)

1. Introduction

This policy provides a framework for the planning, installation, management and maintenance of Closed-Circuit Television (CCTV) systems on sites owned or occupied by Lincolnshire Community Health Services NHS Trust (from here on referred to as 'the Trust') where there is a building management responsibility.

It aims to ensure that appropriate legal requirements are satisfied at each of the above stages and that staff involved in the management and operation of such systems have the necessary information to ensure that they discharge their responsibilities in accordance with the appropriate legislation.

2. Aims and Objectives

CCTV surveillance has become a common feature of our daily lives. Whilst the use of CCTV continues to enjoy general public support, it necessarily involves intrusion into the lives of ordinary individuals in the course of their day to day business. The public expect CCTV to be used responsibly with effective safeguards in place.

The Trust controls a number of CCTV systems on its sites, and it is clear that these systems can assist in the prevention, detection and deterrence of crime, the apprehension and prosecution of offenders, and to provide assurance to staff operation on the sites, particularly those who work alone or are required to work during the hours of darkness.

It is essential that The Trust uses CCTV in a manner that complies with the law and continues to enjoy the support of staff, patients, and the public.

3. Legal Requirements

CCTV systems consist of devices which view and record images of individuals. They also cover other information derived from those images that relate to individuals (for example vehicle registration marks). Therefore the use of CCTV systems is covered by UK Data Protection Legislation, with guidance provided by codes of practice issued by the Information Commissioner's Office (ICO).

UK Data Protection Legislation not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their details, and to claim compensation when they suffer damage as a result of misuse of data.

The basic legal requirements are to comply with UK Data Protection Legislation and the nine Data Protection Principles, thereby ensuring that:

- Those capturing images of individuals comply with the UK Data Protection Legislation;
- The images captured are usable; AND
- Reassurance is available to those whose images are being captured.

The current CCTV Code of Practice can be obtained from ICO at www.ico.gov.uk.

As The Trust's CCTV systems are operated on, or behalf of, a public authority, The Trust also needs to consider wider human rights issues, and in particular, the implications of the *European Convention on Human Rights, Article 8* (the right to respect for one's "private and family life, his home and his correspondence"). This will include assurance that:

- The system is established on a proper legal basis and operated in accordance with the law.
- The system is necessary to address a pressing need, such as public safety, crime prevention or national security.
- It is justified in the circumstances.
- It is proportionate to the problem that it is designed to deal with.

If this is not the case, then it would not be appropriate to use CCTV.

Covert activities of the law enforcement community are covered by *The Regulation of Investigatory Powers Act, 2000* (RIPA). Covert surveillance can only be authorised by the policy, security services, or other agencies empowered by the act. This does not include NHS bodies. Advice on covert surveillance should be sought from the Local Counter Fraud Specialist (LCFS) or Local Security Management Specialist (LSMS).

The Freedom of Information Act, 2000 allows the disclosure of information held by public authorities under certain circumstances; however, data obtained from CCTV systems should only be disclosed, if the disclosure does not breach the Data Protection Principles.

4. Definitions

The following definitions are used throughout this policy:

Approved – Formal confirmation that this document meets the required standards, and may be sent to the Quality Scrutiny Group for ratification.

CCTV – Closed-Circuit Television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited setoff monitors. CCTV systems may use digital or analogue technology, or a mixture of both, and include digital video recorders (DVR), or other media to provide permanent storage.

Stakeholder – An individual or organisation with an interest in the subject of the document: e.g. staff, Staff Side representatives, service users, commissioners.

Surveillance – The monitoring of the behaviour, activities, or other changing information, usually of people, for the purposes of influencing, managing, directing, or protecting.

4.1. Intended Users

Within this policy, where it states "all employees", the definition of which applies to all the employees who are highlighted as followed:

Chief Executive, *Finance Performance and Information*, *Quality*, *Strategy*, *Operations*, *People and Organisational Effectiveness*, *Medical Directorate*, *Council of Governors*.

5. Responsibilities

The **Information Governance Manager** is responsible for:

- Ensuring that all individual CCTV Systems are registered with the ICO;
- Ensuring that each individual system is managed by a named member of staff with the appropriate level of authority;
- Act as the data controller for all of the Trust's CCTV systems;
- Delegate the duties of data controller to the named manager for each discrete CCTV system;
- Advise appropriate staff on all Data protection Act issues relating to CCTV systems;
- Provide advice to authorising senior managers to enable them to make informed decisions on authorisation;
- Take part in the planning and authorisation process for all new CCTV systems;
- Commission periodic audits of CCTV systems to ensure that they remain DPA compliant;
- Investigate any breach of information security in relation to the Trust's CCTV systems.

The **Head of Estates and Facilities Management** is responsible for:

- Ensuring the physical security of the system to ensure that only authorised persons have access to data;
- Ensuring that data requests from law enforcement agencies are referred to the Information Governance Manager and LSMS at the earliest opportunity;
- Reporting all faults in the system;
- Ensuring that each system is serviced at least annually.

The **Local Security Management Specialist** is responsible for:

- Routinely inspecting CCTV systems to ensure that they remain DPA compliant;
- Providing an operational requirement for a;; new CCTV systems in-line with guidance produced by the Home Office, *HOSDB CCTV Operational Requirements Manual, 2009*;
- Providing an operational requirement for all existing CCTV systems where all upgrades or modifications are carried out;
- Measuring progress against the operational requirement on all new works and upgrades;
- Provide assistance and advice on the use of CCTV images following incidents;
- Ensuring the CCTV systems have a maintenance and management contract in place.

The **Head of Service and Operational Managers** have a responsibility to ensure that the policy is implemented within their area and that their teams are aware of the policy and have received appropriate training where necessary. Risk assessments should be raised and managed by the Operational Managers, and it is their responsibility to seek advice where appropriate.

All **Members of Staff** are accountable for their professional practice and hold individual responsibility to be aware of and read policies appropriate to their roles, and others where necessary. They should be aware and comply with their responsibilities within the individual policies of the Trust.

6. Planning new CCTV Schemes

CCTV systems are intrusive and the decision to install CCTV must be informed by a thorough assessment of the problems the system is intended to address. All schemes should be assessed on the impact of people's privacy. This impact assessment process should include the Information Governance Manager, the Estates Manager, the Site Manager, and the LSMS, who should collectively consider the following issues:

- Who will take responsibility for the system and images under the Data Protection Act?
- What is the purpose of the system, and what problems it is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits?
- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objective?
- Is there a need for images of identifiable individuals, or could the scheme use other images not capable of identifying the individual?
- Will the system deliver the desired benefits now, and remain suitable in the future?
- What future demands may arise for wider use of images, and how will these be addressed?
- What are the views of those who will be under surveillance?
- What can be done to minimise intrusion for those who may be monitored?

If justification is found for the new system, the LSMS must produce a statement of overall security need. The LSMS should carry out this work with input for other appropriate staff, and may use the resources of appropriate CCTV installation contractors, particularly if contracts are in place.

Once a system is agreed, it must be authorised by the Health and Safety Committee.

Key stakeholders should work with the LSMS to ensure that the system is procured and installed in accordance with the operational requirement.

7. Management of CCTV Schemes

The local building manager is to ensure that CCTV systems they control operate efficiently, effectively and are maintained to ensure that they continue to meet the operational requirements for the system. Managers of CCTV systems should ensure the following:

- Appropriate signs are prominently displayed on the site to ensure that visitors are aware that they are subject to CCTV surveillance. Signs should be clearly visible and readable, contain details of the organisation, the purpose of the system, and who to contact about the scheme (a telephone number should be sufficient);
- All faults should be reported immediately;
- A deputy should be appointed to ensure that the system continues to be managed in the absence of the manager. The deputy will require appropriate training.
- All staff required to monitor or operate the system are given appropriate training, including periodic training on the Data Protection Act.
- Written local procedures are available for each system. These should include details of those authorised to export data from the system, a plan of all camera locations with camera numbers, manufactures user guides for digital recording devices, and fault reporting procedures;
- An incident report is submitted for any incident involving CCTV system.

Digital and analogue CCTV systems will have a recording device which is connected to all cameras by cable or wireless. This recording device must be secure and only accessible to those authorised to access the data stored on the device.

A retention time of 31 days is accepted to be a reasonable period to retain data. Digital systems will overwrite data based upon the settings programmed into the recorder; however, retention times may be influenced by other restrictions imposed upon the system such as picture quality and image compression. This should be considered when planning and maintaining a system.

Recording devices should have an appropriate media drive to enable the exporting of images to portable media such as DVD. A supply of write-only DVDs should be available with every recording device.

System monitors must be secured and only visible to those authorised to view images. Where the images relate to public areas which are generally accessible and the images merely mirror what can be seen by individuals present in that area there is unlikely to be a problem if a monitor showing these images can be seen by those using the site; however, images from restricted areas should not be visible to the public.

New and established CCTV schemes should only be modified following a thorough review and planning process. This will ensure that the scheme remains DPA compliant. The following are examples of actions that may affect the legal status of a system:

- Changing the field and direction of view of cameras;
- Placing cameras in inappropriate areas, such as toilets, ward sleeping areas, bedrooms, and any other area where higher levels of privacy expected.
- Using systems for covert surveillance without authority.

8. Image Security and Processing

CCTV systems produce images which must be secured at all times. Recording devices, media, and monitors should be secured appropriate. CCTV systems are installed to provide better security and should therefore be used both proactively and reactively to achieve the aims that were intended when the system was installed. This means that images should be available to appropriate, authorised staff and to the law enforcement authorities.

Some members of The Trust's staff who have access to passive monitoring using approved, installed monitors should be able to view images from appropriate cameras. This may include networked CCTV systems using Internet Protocol (IP).

CCTV systems may be used proactively following incidents and can assist with the investigation process; however, any request to view recorded data must be made through the local data controller for the system concerned and where necessary advice should be sought from the Information Governance Manager. Images can only be used for a purpose for which the system was intended. This would cover potential criminal or disciplinary investigations but would not necessarily cover issues of civil liability between individuals such as damage only traffic accidents on NHS property.

Law enforcement agencies routinely request access to appropriate CCTV images when dealing with potential criminal offences. These investigations can be initiated by the Trust, members of staff, patients, or people unconnected with Trust business.

The Police have a right to request access to such information under the Data Protection Act, provided they can show that the information will be used for the prevention and detection of crime, or the apprehension or prosecution of offenders. Data provided must pertain to the investigation.

Where requests are made by the Police, they should be referred to the duty co-ordinator or site manager who should consider the reasonableness of the requests and arrange a time with the Police to export the data requested from the recording device on the production of a formal *Section 29, Data Protection Act* form. If the site manager has any doubts about the request, advice should be sought from the Information Governance Manager, and/or the LSMS before images are provided.

Most requests from the Police can be dealt with during normal working hours, although there may be occasions where urgent access is sought, particularly when dealing with serious crimes. Each site should have an emergency procedure to consider such requests incorporated in the local CCTV procedure.

On every occasion that the Police request to view or copy images, an incident report must be raised, and the Police must sign the *Access to View or Copy CCTV Images* (Appendix C). The form must also be signed by the staff member facilitating the copying of the data, which would likely be the site manager or the LSMS. The Information Governance Manager and LSMS should be informed of the incident and review each individual request. The completed access form should be stored securely, with a copy provided for the Information Governance Manager and the LSMS.

The Police and others legitimately requesting access to images should only be given copies of the original data. Copies should be made onto portable media, such as write-only DVDs and handed over against a signature. Images should not be sent by email or other networked systems. The Police will usually provide their own portable media storage devices.

There may be very rare occasions when the Police require the original recording device, or the hard disk drives from the device. This may be necessary to safeguard forensic data following a serious incident. Site managers should not release recording devices or hard disk drives unless the Police produce a warrant.

Images should only be viewed in a room or area which is secure and allows access only to those authorised to view the data. This requirement should be considered when planning and installing CCTV systems. Special care must be taken at location where there are multiple monitors as it is possible that images replayed on one monitor in a secure room, may also be visible on other monitors on the site which may not be secure.

All media containing CCTV images must be treated as confidential waste if disposal is required. It should be noted that images should only be retained for as long as is necessary to achieve their purpose. Digital media stored on recording devices will be overwritten and VHS tapes, where used, will be recorded over as required by the Data Protection Principles. Data exported from recording devices must be strictly controlled and destroyed when no longer required. The Information Governance Manager can advise further on this issue.

9. Breaches of Policy

Misuse of CCTV equipment and unauthorised processing of data may be criminal offences under the Data Protection Act.

10. Complaints

Any complaints received concerning CCTV systems should be handled in accordance to the *Complaints Policy (P_CIG_08)*.

11. Training

Site managers are to ensure that appropriate members of staff are given adequate training to enable them to operate installed CCTV equipment.

Details of all trained personnel and their responsibilities shall be recorded in local procedures and forwarded to the Information Governance Manager and the LSMS.

Suitable training shall be provided by contractors for all new CCTV systems. Where an existing system is subject to a maintenance agreement, this shall include appropriate training for designated staff.

12. Monitoring Compliance

Site managers are responsible for monitoring compliance with this policy.

The Information Governance Manager shall monitor overall compliance for all of the Trust's CCTV systems.

13. References

This policy was created with reference to the following:

- *CCTV Code of Practice* - published by the Information Commissioner's Office
- *CCTV Operational Requirements Manual, 2009*
- *Data Protection Act, 1998*
- *Freedom of Information Act, 2000*
- *Maintenance of CCTV surveillance systems – code of practice, 2008* - published by the British Security Industry Association
- The Trust's *Information Governance Policy* (at time of initial Policy creation)
- *Equality Act 2010*

Appendix A

Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individuals/group /committee	Frequency of monitoring /audit	Responsible individuals / group / committee (multidisciplinary) for review of results	Responsible individuals / group / committee for development of action plan	Responsible individuals / group / committee for monitoring of action plan
Servicing of Equipment	Premises crime reduction and security management surveys	Local Security Management Specialist	Annual, or more frequent where a risk has been highlighted	LCHS Health and Safety Committee	Local Security Management Specialist	LCHS Health and Safety Committee
Visual checks of cameras and taped information for quality and clarity	Premises crime reduction and security management surveys	Local Security Management Specialist	Annual, or more frequent where a risk has been highlighted	LCHS Health and Safety Committee	Local Security Management Specialist	LCHS Health and Safety Committee
Review Policy	Policy to Committee	Local Security Management Specialist	2 years, or due to significant change in core standards	LCHS Quality Scrutiny Group	Local Security Management Specialist	LCHS Quality Scrutiny Group

Appendix B

Equality Analysis

Title: CCTV Policy (LCHS Owned Sites)
Relevant line in:

What are the intended outcomes of this work? The outcome is to ensure safety for staff, carers and patients. Additionally for monitoring purposes and evidence pending enforcement action.
Who will be affected? Directly affects Directors, Managers and all Members of Staff. Outcomes will affect patients, carers and visitors. Some equipment may be sited in areas that may impact on the wider community if they are involved in activities on Trust premises.

Evidence
What evidence have you considered? None required. The policy and the provisions within apply equally to all persons.
Disability policy applies equally to all persons
Sex policy applies equally to all persons
Race policy applies equally to all persons
Age policy applies equally to all persons
Gender reassignment (including transgender) policy applies equally to all persons
Sexual orientation policy applies equally to all persons
Religion or belief policy applies equally to all persons
Pregnancy and maternity policy applies equally to all persons
Carers policy applies equally to all persons
Other identified groups policy applies equally to all other persons

Engagement and involvement

Was this work subject to the requirements of the Equality Act and the NHS Act 2006 (Duty to involve)? **No**

How have you engaged stakeholders in gathering evidence or testing the evidence available?
None required

How have you engaged stakeholders in testing the policy or programme proposals?
No

For each engagement activity, please state who was involved, how and when they were engaged, and the key outputs:

Summary of Analysis

Eliminate discrimination, harassment and victimisation
N/A

Advance equality of opportunity
N/A

Promote good relations between groups
N/A

What is the overall impact?

The impact will be to ensure the Trust meets its legal obligations in regard to the provision and use of CCTV in its premises.

Addressing the impact on equalities

N/A

Action planning for improvement

Policy to be ratified by the Quality Scrutiny Group
Policy to be approved by the Board
Policy to be updated on the website policies section
Monitoring to take place as detailed in policy
Policy reviewed using NHSLA guidelines

Appendix C

For the record

Name of person who carried out this assessment: Carl Kisby, LSMS

Date assessment completed: May 2016

Name of responsible Director/General Manager: Maz Fosh

Date assessment was signed:

Access to view or copy CCTV images – Police and public

Name of person making request:	

Organisation:	
Address:	
Telephone Number:	

Details of tape to be viewed

Date:			
Reason: (For police only)			
Signed:		Dated:	
Request Granted:		Request Denied (Reason):	

To be completed if tape is removed from circulation

Tape No.	
Issued To:	
Crime No: (For police only)	
Date Issued:	
Issued By:	
Return Date:	

I acknowledge receipt of the above tape:		Date:	
Signed:			