Leicestershire Partnership NHS Trust

CCTV Policy

This policy provides a framework for the planning, installation, management and maintenance of Closed Circuit Television (CCTV) systems on sites owned or occupied by LPT where there is a building management responsibility.

Key Words:	CCTV, Policy	
Version:	4	
Adopted by:	Quality Assurance Committee	
Date Adopted:	13 December 2016	
Name of Author:	Local Security Management Specialist	
Name of responsible committee:	Health and Safety Committee Records Information Governance Group	
Date issued for publication:	September 2019	
Review date:	February 2022	
Expiry date:	1 September 2022	
Target audience:	All Staff	
Type of Policy	Clinical	Non-clinical √
Which Relevant CQC Fundamental Standards?		

CONTRIBUTION LIST

Key individuals involved in developing the document

Name	Designation
Robert Lovegrove	Local Security Management Specialist

Circulated to the following individuals for consultation

Name	Designation
Members	LPT Health and Safety Committee
Members	Directorate Health, Safety and Security Action Group
Sam Kirkland	Head of Data Privacy
Leona Knott	Integrated Equality Service
Kevin Sharkey	Leicestershire Police
Louise Short	Matron (AMH)
Members	Data Privacy Group

Version Control and Summary of Changes

Version number	Date	Comments (description change and amendments)
V1	January 2012	New document
V2	October 2014	Full review and re-write
V2.1	May 2015	Addition of Paragraph 1 to Section 5
V3	August 2016	Reviewed to reflect organisational changes
V4	June 2019	Policy review – Minor changes to reflect current practice

All LPT Policies can be provided in large print or Braille formats, if requested, and an interpreting service is available to individuals of different nationalities who require them.

For further information contact:

Health and Safety Compliance Team
Leicestershire Partnership NHS Trust
Tel: 0116 295 1662
Email: healthandsafety@leicspart.nhs.uk

Definitions that apply to this Policy

All procedural documents should have a definition of terms.

Definitions are a Core Standard

Approved	Formal confirmation that this document meets the required standards and may be sent to the Data Privacy 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 set of 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.
Policy	A policy is principles and rules formulated or adopted by an organisation to reach its long term goals. Policies will be prescriptive by nature. They will state the Trust's expectations for action in a specific subject area and set the parameters within which individuals will operate.
Procedure	Procedures are specific methods employed to express policies in action in date to date operations of the organisation. Together policies and procedures ensure that a point of view held by the organisation is translated into steps that result in an outcome compatible with that view.
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.
Due Regard	Having due regard for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. • Encouraging people from protected groups to participate in public life or in other activities where their participation is disproportionately low.

Contents

Equality Statement

Leicestershire Partnership NHS Trust (LPT) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all.

This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

In carrying out its functions, LPT must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which LPT is responsible, including policy development and review.

Due Regard

LPT must have **due regard** to the aims of eliminating discrimination and promoting equality when policies are being developed. Information about due regard can be found on the Equality page on e-source and/or by contacting the LPT Equalities Team.

The Due regard assessment template is Appendix 6 of this document.

1 Summary

This policy provides a framework for the planning, installation, management and maintenance of Closed Circuit Television (CCTV) systems on sites owned or occupied by LPT 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 Introduction

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.

LPT 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 operating on the sites, particularly those who work alone or are required to work during the hours of darkness.

It is essential that LPT 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 the Data Protection Act 1998 (DPA) with guidance provided by codes of practice issued by the Office of the Information Commissioner (ICO).

The DPA not only creates obligations for organisations, it also gives individuals rights, such as the right to gain access to their data and to claim compensation when they suffer damage.

The basic legal requirements are to comply with the DPA and the eight Data Protection Principles, thereby ensuring that:

- Those capturing images of individuals comply with the DPA;
- The images captured are usable; and
- Reassurance is available to those whose images are being captured.

As LPT 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 private and family life). 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 (RIPA) 2000. Covert surveillance can only be authorised by the police, 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 (FOIA) 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 Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility for all CCTV systems although authority may be delegated to appropriate staff for the planning, procurement, installation, operation and maintenance of CCTV systems.

4.2 Executive Director – Senior Information Risk Owner

The Chief Executive will delegate senior level responsibility for Information Governance within the Trust to the Senior Information Risk Owner (SIRO), an executive director who is responsible for reporting to the Board.

4.3 Head of Data Privacy

The Head of Data Privacy is responsible to the Chief Executive for DPA and FOIA compliance within LPT. The Head of Data Privacy shall:

- Register all individual CCTV systems with the ICO;
- Maintain a log which details the Governance Officer who acts as appoint of contact for each CCTV system;
- Maintain a log of all data access requests for each CCTV system;
- Act as the data controller for all trust CCTV systems;
- Advise appropriate staff on all DPA 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 trust CCTV systems.

4.4 Governance Officers

Governance Officers have a limited role for CCTV systems on LPT premises for which they are assigned. Governance Officers who are responsible for supporting sites with CCTV systems shall:

- Act as local system contact for each CCTV system
- Ensure that only authorised persons have access to data.
- Ensure that data requests received from law enforcement agencies are referred to the Information Request Team via the Head of Data Protection or LSMS at the earliest opportunity;

4.5 Local Security Management Specialist

The Local Security Management Specialist shall:

- Routinely inspect CCTV systems to ensure that they remain DPA compliant;

- Provide an operational requirement for all new CCTV systems in line with guidance produced by the Home Office *(HOSDB CCTV Operational Requirements Manual 2009 (28/09))*;
- Provide an operation requirement for all existing CCTV systems where upgrades or modifications are carried out;
- Measure progress against the operational requirement on all new works and upgrades;
- Provide assistance and advice on the use of CCTV images following incidents;
- Provide advice to authorising senior managers to enable them to make informed decisions on authorisation.

4.6 Data Privacy Group and the Health and Safety Committee

The Data Privacy Group and Health and Safety Committee have responsibility for reviewing and updating the policy as and when legislation changes or every three years if not changes to legislation.

5 LPT CCTV Requirements

It is a requirement under this policy that all new builds and refurbishments include CCTV for all external access/egress, corridors and communal areas with a caveat relating to impact assessment on people's privacy.

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 on people's privacy. This privacy impact assessment process should include the Information Governance Compliance Manager, the scheme project manager the LSMS and appropriate service leads who should collectively consider the following issues:

- Who will take responsibility for the system and images under the DPA
- What is the purpose of the system? What problems is it 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 objectives
- 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 Level 1 and Level 2 operational requirement for the system. The Level 1 operational requirement will define the problem to be addressed and a statement of overall security need; the Level 2 operational requirement will detail the proposed technical specification of the system including: individual camera requirements, operational issues, system requirements and management issues. The LSMS should carry out

this work with input from 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 Chief Executive.

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

Guidance on planning CCTV systems is included at Appendix 2.

6 Management of CCTV Schemes

The governance officers are to promote that CCTV systems they monitor operate efficiently, effectively and are maintained to ensure that they continue to meet the operational requirements for the system, and report faults as identified. They 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 will be sufficient);
- Faults should be reported immediately via the Facilities Help Desk (Telephone: 0116 204 7888, email: facilitieshelpdesk@uhl-tr.nhs.uk or for a NHS Property Services Site; NHS PS Helpdesk 01902 575050 www.property.nhs.uk/fmhelpdesk
- A deputy should be appointed to ensure that the system continues to be monitored in their absence. This is likely to be another Governance Officer covering the area during the absence of the nominated officer;
- 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; manufacturers user guides for digital recording devices and fault reporting procedures;
- An incident report is submitted for any incident involving the 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.

Some analogue systems may still use VHS tapes. Where this is the case these tapes must be securely stored, accounted for and monitored for quality of recording.

A retention time of 30 days is generally 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. These issues should be considered when planning or maintaining a system.

Recording devices should have an appropriate media drive to enable the exporting of images to portable media such as write-only DVD or encrypted USB. 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 as detailed in section 5 of this policy. 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 additional cameras without reviewing the whole system;
- Placing cameras in inappropriate areas such as toilets, ward sleeping areas, bedrooms and any other area where higher levels of privacy are expected;
- Using systems for covert surveillance without authority.

7 Image security and processing

CCTV systems produce images which must be secured at all times. Recording devices, media and monitors should be secured appropriately. However CCTV system are installed to provide better security and should 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 security staff and those 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 governance officer or LSMS and where necessary advice should be sought from the Head of Data Protection. 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, staff or patients or they can be unconnected with trust business.

The police have a right to request access to such information under the DPA provided they can show that the information will be used for the prevention and detection of crime or the apprehension or prosecution of offenders. Clearly data provided must be relevant to the investigation and not amount to a ‘fishing expedition’.

Where requests are made by the police they should be referred to the LSMS or duty co-ordinator who should consider the reasonableness of the request and arrange a time with the police to obtain the data requested from the recording device on the

production of an access form (Appendix 1). During normal working hours the LSMS should be asked to obtain the required data. If requests are received by the Governance Officer or duty co-ordinator advice should be sought from the Head of Data Protection or 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.

On every occasion that the police request to view or copy images the police must sign the access form attached at Appendix 1 to this policy. The form must also be signed by the staff member facilitating the copying of the data which is likely to be the LSMS. The Head of Data Protection, and the LSMS if he/she is not the person facilitating the copying of the data, should be informed of the incident and review each individual request. The original access form must be forwarded to the Information Request Team at the earliest opportunity.

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 DVD or USB and handed over against signature. Images should not be sent by email or other networked systems. The police will usually provide their own portable media.

There may be very rare occasions when the police require the original recording device or a hard disk from the device. Police have a right to seize items under s. 19 of the Police and Criminal Evidence Act 1984 (PACE) if they believe that this may be necessary to safeguard forensic data following a serious incident. They do not require a warrant in these circumstances but must justify this action in each case. If this occurs the Director on Call must be notified immediately and the provision of replacement hardware considered.

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 Head of Data Protection can advise further on this issue.

8 Information Requests

Any information requests for data under the FOIA or DPA concerning the processing of images should be referred to the Head of Data Privacy. Further information on subject access requests is available in the Confidentiality, Caldicott and Data Privacy Policy, FOI Policy and FOI Operational Procedure.

9 Breaches of this policy

Misuse of CCTV equipment and unauthorised processing of data may be criminal offences under the DPA or other legislation.

10 Complaints

Any complaints received concerning CCTV systems should be handled in accordance with the Trust's Complaints Policy.

11 Training

There is no training associated with this Policy.

12 Monitoring

The Health and Safety Committee will monitor compliance by receipt of quarterly reports from the Local Security Management Specialist which will include details of Crime Reduction and Security Surveys undertaken.

The Data Privacy Group (DPG) shall monitor overall compliance for all LPT CCTV systems.

13 Review of Policy

The Trust will review the policy every three years to reflect any organisational changes, national guidance or changes in legislation.

14 Publicising this Policy

This Policy will be a document available electronically on the Trust's Intranet site.

15 References and Associated Documentation

This policy was drafted with reference to the following:
The CCTV Code of Practice www.ico.gov.uk
CCTV Operational Requirements Manual (28/09) www.nactso.gov.uk
UK Police Requirements for Digital CCTV Systems (09/05) www.nactso.gov.uk
Data Protection Act 1998 www.legislation.gov.uk
Freedom of Information Act 2000www.legislation.gov.uk
BSIA maintenance and servicing of CCTV surveillance systems (2008) www.bsia.co.uk
BS EN 50132-7:1996 European Standards for CCTV Systems www.standardsuk.com
Information Governance Management Strategic Framework Policy and Strategy
Confidentiality, Caldicott and Data Protection Policy
Data Protection Policy
FOI Policy
FOI Operational Procedure
Information Security Policy
Records Management Strategy
Information Lifecycle and Records Management Policy
Equality Act 2010

Appendix 1

Leicestershire Partnership NHS
NHS Trust

ACCESS TO VIEW OR COPY CCTV IMAGES – POLICE AND PUBLIC

Please advise the person making the request that at least 24 hours' notice is required for all requests. Requests made on weekends or Bank Holidays will be actioned on the next working day (Monday – Friday).

Name of person making request:	
Organisation:	
Address:	
Telephone Number:	

DETAILS OF TAPE TO BE VIEWED

Date:	
Reason: (For police only)	

Form to be forwarded to: lptsecurity@leicspart.nhs.uk

Signed:		Dated:	
Request Granted:		Request Denied (Reason):	

TO BE COMPLETED IF TAPE 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:			

Once complete please forward request to: lpt-SARRequests@leicspart.nhs.uk

GUIDANCE ON THE PLANNING OF CCTV SYSTEMS

Planning of CCTV Systems for LPT

This appendix is intended as a guide to project staff and any final decisions on CCTV installations should be agreed by project and clinical staff to ensure that the interests of all are taken into consideration.

CCTV systems in hospital areas can be considered in three areas:

Public areas – these are areas of the hospital to which the public have unrestricted access. These areas can be both internal and external and include: grounds, access roads, car parks, egress and access points, reception and waiting areas. For the purposes of this document they include all public areas up to the access and egress point to wards.

Communal areas – these are parts of a ward or other closed healthcare facility shared by all patients. They include day rooms, dining areas and corridors.

Private areas – these are those areas where any individual might reasonably expect privacy. These include: bathrooms, bedrooms, toilets, consulting and interview rooms and seclusion rooms.

Advice on the installation of CCTV resources by area is shown in the table below.

Area	CCTV resources
Public areas	CCTV is commonly in use in public areas of hospitals. There are no special considerations required for hospital beyond those placed by the Information Commissioner on all CCTV cameras, such as signage, notification, etc. In LPT this is not controversial. External areas around buildings, access and egress points, reception and waiting areas should generally be monitored if natural surveillance is poor or it is deemed appropriate due to the risks associated with criminal behaviour on the site.
Communal areas	CCTV to be used in communal areas where the safety of service users, staff or the public is believed to justify this. It is central to any decision that, in line with the requirements of the Information Commissioner, a clear reason for installation is available. (Risk assessments and incident reports should be used to support CCTV systems) In LPT CCTV resources have only recently been included within ward areas, including access and egress points, corridors, garden areas and day rooms. Older wards do not have CCTV resources. It is a requirement under the policy that new and replacement systems will include as near 100% coverage as possible of these communal areas. This would include dining areas,

	sitting rooms and other shared resources with caveat relating to impact assessment on people's privacy.
Private areas	The legal basis for using CCCTV in private spaces arises from the patient's capacitated consent or because such monitoring is an agreed and appropriate part of compulsory treatment (for patients detained under the Mental Health Act 1983) and is proportionate in an individual case. This means that while it may be legal to use cameras in bedrooms, seclusion rooms and toilets, there would be a considerable burden on the provider to prove that the intrusion was proportionate. It is also arguable that the burden would be higher still if the cameras are linked to a recording device, rather than providing real-time unrecorded images. The General Medical Council has provided guidance on making and using visual and audio recordings of patients: Making and Using Visual and Audio Recordings of Patients (May 2002). Very great care needs to be taken in the siting off the monitors to ensure that there is no inappropriate deliberate or accidental viewing of images by patients, staff or visitors to the ward. Particular consideration also needs to be given to issues of gender, and whether use of CCTV cameras in private areas provides any potential for increasing patient vulnerability, inappropriate behaviour, sexual harassment or abusive relationships. All decisions on CCTV in private areas must be made in consultation with clinicians and a robust, documented, authorisation process carried out. Questions of legality should be made after consulting the Information Commissioner, the GMC and other appropriate legal resources.

Monitored activity – types of activity that are commonly monitored are:

- Theft and criminal damage
- Staff, patient and public safety (including violence and aggression)
- Access and egress
- Movement on site (externally and internally)
- Antisocial behaviour and vandalism.

The purpose of observation – Consider how much detail is required in the monitored image. It may be necessary to:

- Monitor a large area
- Detect individuals approaching a building
- Observe the actions of a group of people
- Recognise known individuals at an entrance.

The purpose for which a camera is installed will determine the field of view of the camera, the frame rate of the recorded images and the level of detail recorded (image quality, compression).

Many cameras are ineffective because they are poorly sited and consideration has not been given to the purpose for which the camera is intended. The LSMS can advise further on this as part of the operational requirement stage.

Recording of Images – are currently recorded on digital video recorders (DVR). These recorders can be connected to the cameras using coaxial cables, twisted pair cable or wireless. It is important that these devices are secure and tamper proof. Whilst public and communal areas can be connected to the same DVR, private areas, where there is a recording requirement, should be connected to a separate secure DVR.

DVRs should be secured in a lockable cabinet and the keys held securely away from the ward. PIN numbers on all DVRs should be changed from the default setting and have an individual, unique PIN set. Separate PINs should be used for searching and recording data. Ideally DVRs should be secured in areas where they are not accessible to maintenance staff, so roof voids should be avoided. It is better that they are secured in the ward but in an area that cannot be accessed by staff and patients and therefore the DVR should not be able to be removed without authority.

All new systems should employ high definition (HD) cameras and be connected to the data network. This should only be carried out in accordance with the IT Security Policy. Networking can be configured either by connecting DVRs to the network or by connecting cameras to a switch which is then connected to a data storage area such as a server. Data can be accessed by nominated staff using proprietary software installed on PCs. It is suggested that Duty Coordinators or Managers, the LSMS and other appropriate nominated staff could do this when authorised to do so. Ward staff should be able to see certain cameras on monitors but should not under any circumstances be able to view or copy recorded data without authority.

Appendix 3

Policy Monitoring Section

Reference	Minimum Requirements to be monitored	Evidence for self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	All CCTV systems are currently registered with ICO		SIRO requires assurance from IG Manager.	IG Manager	Annually
	Physical security of system Access to data		Governance Officer Risk Assessments Crime Reduction Surveys Review incident reports	Health and Safety Committee via LSMS	Quarterly
	Physical security of system	Annual check	A planned preventative maintenance (PPM) via contract with ADT	Estates and Facilities Management	Quarterly
	The process for access to data by authorised persons is followed	Single Point of Access - Information Requests Team	IRT logged on Safeguard and will be included report	Data Privacy Group	Six monthly report

Appendix 4

Leicestershire Partnership NHS
NHS Trust

The NHS Constitution

NHS Core Principles – Checklist

Please tick below those principles that apply to this policy

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	☐
Respond to different needs of different sectors of the population	√
Work continuously to improve quality services and to minimise errors	☐
Support and value its staff	√
Work together with others to ensure a seamless service for patients	☐
Help keep people healthy and work to reduce health inequalities	√
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	☐

Appendix 5

Due Regard Screening Template

Section 1	
Name of activity/proposal	CCTV management and use
Date Screening commenced	October 2014
Directorate / Service carrying out the assessment	Health and Safety Compliance Team
Name and role of person undertaking this Due Regard (Equality Analysis)	Samantha Roost, Senior Health and Safety Advisor
Give an overview of the aims, objectives and purpose of the proposal:	
AIMS: The aim of this policy is to provide a framework for the planning, installation, management and maintenance of Closed Circuit Television (CCTV) systems on sites owned or occupied by LPT where there is a building management responsibility.	
OBJECTIVES: Provide CCTV systems for the prevention and detection of crime	
PURPOSE: To establish mandatory requirements for the management of ventilation systems	

Section 2		
Protected Characteristic	**Could the proposal have a positive impact Yes or No (give details)**	**Could the proposal have a negative impact Yes or No (give details)**
Age	No	No
Disability	No	No
Gender reassignment	No	No
Marriage and Civil Partnership	No	No
Pregnancy and Maternity	No	No
Race	No	No
Religion and Belief	No	No
Sex	No	No
Sexual Orientation	No	No
Other equality groups?		

Section 3			
Does this activity propose major changes in terms of scale or significance for LPT? For example, is there a clear indication that, although the proposal is minor it is likely to have a major affect for people from an equality group/s? Please tick appropriate box below.			
~~Yes~~		**No**	
High risk: Complete a full EIA starting click here to proceed to Part B		Low risk: Go to Section 4.	

Section 4
It this proposal is low risk please give evidence or justification for how you reached this decision:

Sign off that this proposal is low risk and does not require a full Equality Analysis:
Head of Service Signed: Bernadette Keavney

Date: 29/08/2019

Appendix 6

Policy Training Requirements

The purpose of this template is to provide assurance that any training implications have been considered

Training topic:	CCTV Policy
Type of training:	Mandatory (must be on mandatory training register) √ Role specific Personal development
Division(s) to which the training is applicable:	√ Enabling Services
Staff groups who require the training:	Staff within the Data Privacy Team may need training in the process and implementation of the policy when a request has been received
Update requirement:	N/a
Who is responsible for delivery of this training?	Data Privacy Lead
Have resources been identified?	N/a
Has a training plan been agreed?	N/a
Where will completion of this training be recorded?	Personal File Other (please specify)
How is this training going to be monitored?	Via Annual Review

Appendix 7

PRIVACY IMPACT ASSESSMENT SCREENING

Privacy impact assessment (PIAs) are a tool which can help organisations identify the most effective way to comply with their data protection obligations and meet individual's expectations of privacy. The first step in the PIA process is identifying the need for an assessment.

The following screening questions will help decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise and requires senior management support, at this stage the Head of Data Privacy must be involved.

Name of Document:	CCTV		
Completed by:	Bernadette Keavney		
Job title	Head of Trust Health and Safety Compliance	**Date**	29/08/19

	Yes / No
1. Will the process described in the document involve the collection of new information about individuals? This is information in excess of what is required to carry out the process described within the document.	**No**
2. Will the process described in the document compel individuals to provide information about themselves? This is information in excess of what is required to carry out the process described within the document.	**No**
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information as part of the process described in this document?	**No**
4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	**No**
5. Does the process outlined in this document involve the use of new technology which might be perceived as being privacy intrusive? For example, the use of biometrics.	**No**
6. Will the process outlined in this document result in decisions being made or action taken against individuals in ways which can have a significant impact on them?	**No**
7. As part of the process outlined in this document, is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For examples, health records, criminal records or other information that people would consider to be particularly private.	**No**
8. Will the process require you to contact individuals in ways which they may find intrusive?	**No**

If the answer to any of these questions is 'Yes' please contact the Head of Data Privacy Tel: 0116 2950997 Mobile: 07825 947786
Lpt-dataprivacy@leicspart.secure.nhs.uk
In this case, adoption n of a procedural document will not take place until approved by the Head of Data Privacy.

IG Manager approval name:	
Date of approval	

Acknowledgement: Princess Alexandra Hospital NHS Trust