Cumbria Partnership NHS
NHS Foundation Trust

Closed Circuit Television Policy

Document Summary

To state the Trust's policy for ensuring, CCTV is sited, operated, used for investigation purposes and monitored appropriately, and that Statutory requirements of the Data Protection Act 1988 and Human Rights Act are adhered to.

POLICY NUMBER	POL/002/061
DATE RATIFIED	April 2016
DATE IMPLEMENTED	April 2016
NEXT REVIEW DATE	April 2019
ACCOUNTABLE DIRECTOR	Director of Strategy and Support Services, Executive Lead and Accountable Officer for Finance
POLICY AUTHOR	Safety and Security Officer

Important Note:
The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and, as such, may not necessarily contain the latest updates and amendments.

Table of Contents

1. Scope 3
2. Introduction 3
3. Statement of Intent 4
4. Legal Requirements 5
5. Definitions 6
   - 5.1 Description 6
   - 5.2 Type of Data and Purpose of Use 6
   - 5.3 Third Parties 7
   - 5.4 Appropriate and Effective Use 7
   - 5.5 Public Place 7
6. Duties 8
   - 6.1 The Chief Executive 8
   - 6.2 Senior Information Risk Owner (SIRO) 8
   - 6.3 Head of Information Governance 8
   - 6.4 Estates, Facilities and Capital Investment Manager 8
   - 6.5 Professional Head of Estates 9
   - 6.6 Local Security Management Specialist (LSMS) 9
   - 6.7 Ward / Unit / Department Managers 9
   - 6.8 Trust Staff 9
7. Arrangements / Detail 9
   - 7.1 Management of CCTV Schemes 10
   - 7.2 Management Review 11
   - 7.3 Record Keeping and Monitoring 11
   - 7.4 Health and Safety Considerations 12
   - 7.5 Installing CCTV 12
   - 7.6 Selecting, Siting and Using Cameras 12
   - 7.7 Use of CCTV in Inpatient Units 13
   - 7.8 Covert Recording 14
   - 7.9 Signage 14
   - 7.10 Storage and Viewing 15
   - 7.11 Disclosure 15
   - 7.12 Quality of Images 17
   - 7.13 Image Security and Processing 18
   - 7.14 Law Enforcement Agencies 18
   - 7.15 Retention and Disposal of Images 18
   - 7.16 Dissemination and Implementation 19
8. Training 19
9. Monitoring Compliance with this Policy 19
10. References / Bibliography 20
11. Related Trust Policy / Procedures 20

Appendix 1 – ICO Registration 22

Appendix 2 – CCTV Checklist 23
Appendix 3 – Location of CCTV Cameras and Signage 25
Appendix 4 – Cumbria Partnership NHS Foundation Trust Closed Circuit *(CCTV) Systems Information Leaflet* 26

1. Scope

This policy details how Cumbria Partnership NHS Foundation Trust (CPFT) will maintain and operate Closed Circuit Television (CCTV) cameras within designated Trust facilities throughout Cumbria. It also details the procedures to be used for recording, retaining and using information obtained from the use of the CCTV system installed throughout Trust facilities within Cumbria.

CPFT has an estate of mixed-use facilities including community hospitals, mental health in-patient units, clinics, and other buildings, some or all of which allow or include access/admission of members of the public as well as patients, CPFT Staff and Bank / Voluntary Staff members. In addition, other persons may come into contact with CPFT CCTV systems such as employees of companies either directly or indirectly dealing with, or trading with, CPFT.

It is necessary therefore to have a policy that includes a set of procedures on the use, retention and subsequent analysis of any such CCTV system, in use within CPFT. This policy will enable all persons who use, or come into contact with, CCTV recording equipment, to be reassured that it is being used in the correct manner.

2. Introduction

The CCTV policy applies to all staff within the Cumbria Partnership NHS Foundation Trust and other persons working within the organisation that may for whatever reason, be present on Trust premises. It also has particular relevance for those members of staff who have a responsibility for using or managing CCTV systems, or acting as the Trust point of contact for enquiries.

This policy is compliant with The Human Rights Act 1998, The Data Protection Act 1998, 'In the Picture: A data protection code of practice for surveillance cameras and personal information' produced by the Information Commissioner's Office, the Caldicott Principles and the Regulation of Investigatory Powers Act 2000.

CCTV has become a part of every-day life for the vast majority of the population of Great Britain. CPFT, like so many other organisations, employs the use of CCTV in many of its buildings both for security purposes and, in the case of CCTV within in-patient areas, as a further measure to safeguard both patients and staff.

As well as providing important safeguards, the use of CCTV also enhances public confidence, and allows for the recording, storing and retrieval of information over an extended period of time.

The use of surveillance systems within clinical environments is not intended as a substitute to or to replace security vigilance and local management. The use of the systems is intended to support staff and services to promote a safer environment.

It is now well accepted that CCTV within in-patient areas, can be a useful tool to assist in the monitoring of vulnerable patients and thereby help reduce the instances of self-harm. However, the use of cameras in what might normally be regarded as an area where a patient can expect an element of privacy raises some human rights issues. It is vital therefore that any invasion of the right to privacy is balanced appropriately and sensitively with the need for Trust staff to effectively discharge their duty of care to persons who are in care and who are at increased risk of harm.

The policy does not replace or remove any statutory obligations on operators or users of such systems to comply with the provisions of the following legislation:

- Data Protection Act 1998;
- Human Rights Act 1998; and
- Regulation of Investigatory Powers Act 2000 (RIPA).

This policy is set to inform all users of the Trust that the use of data in the form of images is being recorded onto secure digital recording systems. All users must be assured that compliance with the principles of the Data Protection Act relating to information handling that is legally enforceable has been adopted and is managed by the Trust. The Act requires the Trust to ensure that:

- Data is obtained and processed fairly and lawfully.
- Data is held only for the purposes specified in the ICO registration (Appendix 1).
- Data is used only for the purposes listed in the registration and only disclosed to those organisations listed and to individuals in relation to their personal information and their rights under the Act, unless the Act provides an exemption.
- Subject matter does not conflict with issues of medical confidentiality, e.g. recording images of persons attending sexual health clinics.

The purpose of using subject matter is to support the following:

- Providing assistance in the prevention, deterring and detecting of crime.
- Helping to identify, apprehend and prosecute offenders.
- Providing the Police and the Trust with evidence to take criminal and civil action in the courts.

3. Statement of Intent

The principal intent of this policy is to identify and implement CCTV responsible practices and procedures in order to assist in the overall protection of all staff service users and visitors.

This can be achieved by a combination of improved working practices, greater staff education, awareness and involvement and an ongoing commitment to the pursuance of technical improvements. In particular, the Trust aims to:-

- Encourage the legal efficient and effective use of the technology available.
- Ensure that CCTV systems strengthen CPFT's position of compliance with current and future Data Protection and Human Rights legislation.
- Instil and maintain public confidence in the use of CCTV systems.
- Act in partnership with Trust and other agencies / businesses in the approach to CCTV, thereby increasing public confidence through open and effective partnerships.
- Promote the adoption of clear, well recognised standards for CCTV that command public confidence.
- Moreover, these aims should complement the key principles behind any scheme, notably Data Protection, Human Rights, Public Interest, Accountability and Privacy.

4. 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 CPFT 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 nation 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 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.

5. Definitions

5.1 Description

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted.

5.2 Type of Data and Purpose of Use

Prior to considering compliance with the principles of the Data Protection Act (DPA), a user of CCTV or similar surveillance equipment, will need to determine two issues which are:

5.2.1 Personal data is where the data relates to a specific individual of which the individual is identified or identifiable in the hands of a recipient of the data, from this data alone or used with other information which is in the possession of, or is likely to come into the possession of the recipient. Personal data includes:

- Name;
- Address;
- Date of birth;
- National insurance number;
- Credit card number;
- Passport number;
- Blood group;
- DNA, shoe size;
- Favourite restaurant;
- Sexual preference;
- Destination of air travel;
- Medical history;
- Geographical location; and
- Last time and or place credit card used.

5.2.2 The type of personal data being processed, i.e. is there any personal data which falls within the definition of sensitive personal data as defined by Section 2 of the DPA; Sensitive personal data' includes:

- Ethnic origin or race;
- Political opinion;
- Religious or other beliefs of a similar nature
- Trade Union membership;
- Health – mental or physical;
- Sexual orientation;
- Commission of any offence (or alleged); and
- Any court proceedings or findings.

5.2.3 The purpose(s) for which both personal and sensitive personal data is being processed.

5.2.4 The Information Commissioner will take into account the extent to which users of CCTV and similar surveillance equipment have complied with this Policy when determining whether they have met their legal obligations when exercising their powers of enforcement.

5.3 Third Parties

In the context of CCTV footage, this refers to any person, persons or organisations other than relevant Trust staff and the individual/s that are captured on the image or footage who may wish to view or seize it e.g. Trust, solicitors or media.

5.4 Appropriate and Effective Use

This refers to the usefulness of the deployment of the CCTV system and it being used for its intended purpose e.g. a camera pointed at a disused car park would not be effective use whereas facing a busy reception area entrance would be.

Wherever possible, alternative methods of problem solving should be considered before installation of CCTV. This will be done on an individual risk assessment basis.

CPFT use overt CCTV cameras, which can be recorded onto video tape (generally for coverage of exterior areas and areas open to the general public) or for recording onto a digital recording medium i.e. Hard Drive, Compact Disc (CD). None of the CCTV cameras in use record in audio.

5.5 Public Place

Public place is defined in Section 16(b) of the Public Order Act 1986 and is taken to include any highway and any place to which at the material time the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission.

6. Duties

6.1 The Chief Executive

CPFT is the data controller for all captured CCTV information and is registered with the Information Commissioners Office.

The Chief Executive assumes overall responsibilities for ensuring CCTV installations uses and data control are effectively addressed within the Trust although authority may be delegated to appropriate staff for the planning, procurement, installation, operation and maintenance of CCTV systems.

The Director responsible for policy implementation is the Director of Strategy and Support Services, Executive Lead and Accountable Officer for Finance, as the Trust's designated Security Management Director.

6.2 Senior Information Risk Owner (SIRO)

The SIRO (Director of Strategy and Support Services, Executive Lead and Accountable Officer for Finance) is responsible for Leading and fostering a corporate culture that values, protects and uses information for the success of the organisation and benefit of people who use our services. The SIRO is responsible for advising the Chief Executive on the information risk aspects of their statement on internal controls

6.3 Head of Information Governance

The Head of Information Governance holds the responsibility of registering all data collection methods, including CCTV, with the Information Commissioner's Office and for all liaisons with the Information Commissioner. This individual also holds responsibility for providing authorisation for any requested sighting / downloading / sharing of CCTV recordings with a third party.

The Head of Information Governance is also a source of information regarding confidentiality and compliance issues.

6.4 Estates, Facilities and Capital Investment Manager

The Estates, Facilities and Capital Investment Manager is the Information Asset Owner (IAO) and as such holds records of all CCTV systems in use on an asset register.

The Trust's Estates Department is responsible for the initial acquisition and installation of all CCTV systems in use by CPFT, and also for any major refurbishment programme to update or improve existing systems.

6.5 Professional Head of Estates

The Professional Head of Estates is the asset administrator and ensures ongoing maintenance and upkeep of all CCTV systems and maintains the asset register.

6.6 Local Security Management Specialist (LSMS)

The LSMS is the Trust's Safety and Security Officer and is responsible for providing advice on the provision of access and material to law enforcement agencies including the police, as well as advising on the provisions of the CCTV Code of Practice and the provision of new or additional CCTV equipment, in collaboration with the Head of Information Governance. The LSMS is furthermore responsible for:-

- Liaising with the Professional Head of Estates to ensure all appropriate statutory requirements in relation to the Trust's use of CCTV are being adhered to.
- Providing advice to Trust staff regarding impact risk assessing and, where CCTV is deemed necessary, the appropriate sighting and use of CCTV.
- Liaising with Trust or other agencies regarding access to recordings and protection of information.

6.7 Ward / Unit / Department Managers

When considering installation of CCTV, Ward / Unit / Department Managers should firstly undertake an impact risk assessment in conjunction with the LSMS to determine if alternative solutions which are less invasive can be put into place.

Ward/Unit/Department Managers must ensure the Professional Head of Estates is included in any discussions for the potential installation of CCTV.

Where CCTV is in place, the responsibility for monitoring the recording, storage, and retrieval of CCTV images will lie with Ward / Unit /Department Managers as part of the operation and day-to-day usage of CCTV systems under their control.

It is their duty to ensure that all staff operate within the confines of this policy and are appropriately trained.

It is their responsibility to seek advice and guidance from the Head of Information when requests are made in relation to access and the Head of Information and/or the LSMS should they have queries regarding any other aspect of CCTV.

6.8 Trust Staff

All staff involved in the use of CCTV installations will ensure they operate the systems in accordance with Trust policy and statutory requirements. All staff will receive training appropriate to their activities and responsibilities relating to CCTV operations.

7. Arrangements / Detail

7.1 Management of CCTV Schemes

The Professional Head of Estates will ensure that the CCTV systems they monitor operate efficiently, effectively and are maintained to ensure that they continue to meet the operational requirements for the system. 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.
- All faults should be reported immediately.
- All staff required to monitor or operate the system are given appropriate training, including periodic training on the DPA;
- 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.

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

Recordings should be disposed of after 31 days in accordance with the Trust's procedures using appropriate companies.

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 example 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.

7.2 Management Review

A review of local CCTV management will be undertaken as part of a rolling programme of site audits. A review of CCTV Management System will be undertaken periodically by the LSMS and include:

- Results from audits (where undertaken);
- The extent to which CCTV is in use;
- Review of risk assessments;
- Review of asset register and maintenance programme;
- Review of complaints and requests; and
- Review of training records.

The review will culminate in a report on the use of CCTV to the Corporate Fire, Health, Safety and Security Committee.

7.3 Record Keeping and Monitoring

Records will be maintained by the Professional Head of Estates for the following:

- Type of CCTV installation;
- Location of CCTV installation;
- Number and location of cameras operating within the system;
- Procedure for use and monitoring of data held by the system;
- CCTV equipment maintenance log.

Staff training records will be held by Workforce and Organisational Development.

Any information requests for data under the Freedom of Information Act 2000 or Data Protection Act 1998 concerning the processing of images should be referred to the Head of Information Governance. Further information on subject access requests is available in the Data Protection Act Policy and Freedom of Information Act Policy.

Any complaints received concerning CCTV systems should be handled in accordance with the Trust's Dealing with Complaints and Comments Policy and also directed to the Head of Information Governance.

The purpose of the scheme is to protect the vital interests of the patient; the right to serve a notice to request removal of a camera does not apply. If such a notice is received, a reply must be given within 21 days, either indicating an intention to comply with it or giving an explanation as to why the notice is not justified. If such a request is granted, the camera(s) should be either covered up or removed.

7.4 Health and Safety Considerations

The design and operation of CCTV systems must take full account of the statutory requirements contained in the Health and Safety (Display Screen Equipment) Regulations 1992 as CCTV monitors are classed as 'display screen equipment' and therefore fall within the remit of these Regulations. Prolonged monitor viewing should be avoided; operators should not look at CCTV monitors for long periods without either a rest break or alternative task activity.

7.5 Installing CCTV

CPFT staff should ensure that when installing CCTV the problem they are trying to address has been clearly defined and installing cameras is the best solution. The decision to install cameras should be reviewed on a regular basis as determined by the Information Asset Owner (IAO).

CPFT staff should ensure the completion of CCTV systems checklist when installing new surveillance equipment. (Appendix 2)

The checklist should be reviewed on a regular basis in conjunction with the review of the system.

7.6 Selecting, Siting and Using Cameras

Camera selection needs to be based upon its usage. Usage falls into four categories and will require different types of system for each circumstance. These categories are:

- **Monitoring:** to watch the flow of traffic or the movement of people where you do not need to pick out individual figures.
- **Detecting**: to detect the presence of a person in the image, without needing to see their face.
- **Recognising:** to recognise somebody you know, or determine that somebody is not known to you.
- **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

Cameras shall not be hidden but should as far as is consistent with the purposes of the scheme be placed in public view.

The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment.

Cameras have been positioned to avoid capturing the images of persons not visiting the premises.

Cameras should not observe clinical or treatment areas where patient dignity or confidentiality may be compromised, nor should they have sight of any private premises

without the express written permission of the owner of those premises unless they come into view as part of a wide-angle or long-shot only.

It is important that a CCTV system produces images that are of a suitable quality for the purpose for which the system was installed. If identification is necessary, then poor quality images which do not help to identify individuals may undermine the purpose for installing the system.

The following principles apply when considering camera location: (see Appendix 3)

- Place the camera in a location to minimise viewing spaces that are not of relevance to the purposes for which you are using CCTV.
- Ensure that the choice of cameras to be sited can produce images of the right quality, taking into account their technical capabilities and the environment in which they are placed.
- The camera must be suitable for the location, bearing in mind the light levels and the size of the area to be viewed
- Cameras must be sited so that they are secure and protected from vandalism.
- The system must produce images of sufficient size, resolution and frames per second.

In areas where people have a heightened expectation of privacy, such as changing rooms or toilet areas, cameras should only be used in the most exceptional circumstances where it is necessary to deal with very serious concerns. In these cases, you should make extra effort to ensure that those under surveillance are aware (see section 7.9).

The cameras should be protected from vandalism, and a maintenance log should be held for each camera. If a camera is damaged, there should be clear procedures for defining the person responsible for making arrangements for ensuring the camera is fixed within a specific time period and monitoring the quality of the maintenance work.

7.7 Use of CCTV in Inpatient Units

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.

The introduction of CCTV to inpatient units should be given careful consideration, as it may not be in inpatients' best interests. The use of CCTV should be considered on an individual patient basis, based on risk and clinical assessments. Patients may consider CCTV intrusive and, in certain circumstances, it could have a negative effect on a patient's mental state.

Article 8 of the European Convention on Human Rights affords 'the right to respect for private and family life'. It can, however, be interfered with by a public authority for the' protection of health'. It is not uncommon for certain patient groups to be subject to regular monitoring that is consistent with their care plan but which clearly deprives them of an

element of privacy. This may take the form of door openings or lights on, and, in certain circumstances, CCTV, which may result in less interference with the patient from staff.

If a decision is made to install CCTV in patient areas, or new patients enter a ward, staff, patients and visitors must be advised of the system and the potential benefits it can offer over traditional systems. While a patient's consent is preferable, it is not required when the purpose of the system is considered to be in their best interests.

7.8 Covert Recording

This policy does not allow covert surveillance or any activity that would be considered covert surveillance as defined in the Regulation of Investigatory Powers Act 2000 (RIPA). The use of covert video or audio devices by NHS organisations when tackling any type of criminal activity will need a RIPA authorisation from the Police. If the request through the police is refused then authority can only be given by NHS Protect. For further advice and guidance contact the Trust Local Security Management Specialist.

Any surveillance that is used in a non-public place for the purpose of capturing more sensitive personal data about an individual is likely to require explicit consent of that individual to be lawful. This is also the case when gathering information that is particularly intrusive of a person's privacy (even where it is not the specific intention to do so)

Particular consideration also needs to be given to issues of gender, and whether the use of CCTV cameras provides any potential for increasing patient vulnerability, inappropriate behaviour, sexual harassment or abusive relationships.

Information obtained or recorded through the use of surveillance must be kept secure, and anyone with authorised access to that information must understand their legal responsibilities.

7.9 Signage

Prominently placed signs at the entrance to the CCTV zone are displayed where CCTV is in use. These are reinforced with further signs inside the area. CCTV signs shall inform the public that cameras are in operation and allow people entering the car park / hospital / clinic etc. to make a reasonable approximation of the area covered by the scheme.

Signage used must be:

- Clearly visible and readable.
- Contain details of the organisation operating the system, the purpose for using CCTV and who to contact about the scheme (where these things are not obvious to those being monitored); and;
- Be an appropriate size depending on context, for example, whether they are viewed by pedestrians or car drivers.

With this in mind, the size of the signs may vary according to circumstances, e.g. a sign on entrance door to a building or in corridors may only need to be A4 size, whereas signs at entrances of sites and car parks alerting drivers/pedestrians to the fact that the site and car parks are covered by such equipment will normally need to be larger, for example A3 size as they are likely to be viewed from farther away.

Signs placed within departments and wards should be A5 size.

All signs should state the Trust's name and set out the purpose of which CCTV cameras are being used and contact details for further information.

7.10 Storage and Viewing

If tapes, recordable discs or hard drives are used, they are to be of suitably good quality and should be securely stored. The medium on which images are captured should be saved then removed so images are not recorded on top of images recorded previously. The medium on which the images are recorded should not be used when it has become apparent the quality of images has deteriorated or become corrupted.

Viewing of live images on monitors should usually be restricted to the operator unless the monitor displays a scene which is also in plain sight from the monitor location.

Monitors which display images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised staff (this would apply to seclusion room). Cross-refer to policies applicable to seclusion room.

Viewing of recorded images should take place in a restricted area and no unauthorised personnel should be allowed access when viewing is taking place. If tapes are watched, a report should be made to include the date, time, who was viewing, why, the outcome, if any, of the viewing and the date/time the images were returned to secure storage. A local documented procedure for ensuring the accuracy of this information must be maintained.

Recorded material must not be sold or used for commercial purposes or the provision of entertainment. All images which are digitally recorded will be stored securely within the systems hard drives and automatic erasure takes place after 31 days.

7.11 Disclosure

7.11.1 General

Disclosure of images from CCTV systems 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 is appropriate to disclose images to law enforcement agencies where a crime needs to be investigated, but it would not be appropriate to disclose images of identifiable individuals to the media for entertainment purposes or place them on the internet.

NOTE: Even if a system was not established to prevent and detect crime, it would 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. Data provided must be relevant to the investigation and not amount to a 'fishing expedition'.

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.

The Caldicott Guardian may need to be consulted before disclosure of information is granted.

The product/data should only be handed to the police or any other party after authority has been obtained from the Head of Information Governance or a nominated deputy in line with the requirements of the Data Protection Act 1998.

The downloading of images is a specialist task, and may only be undertaken by personnel who are trained to do so and authorised by the Head of information Governance or a nominated deputy in line with the requirements of the Data Protection Act 1998.

Medium containing the recorded images for viewing purposes or for use in legal proceedings should be documented and a signature of the viewer or collecting officer obtained. A local documented procedure for ensuring the accuracy of this information must be maintained.

7.11.2 Data Protection Act 1998 / Subject Access Requests

Section 7 of the Data Protection Act 1998 affords data subjects the right to access copies of media on which their image may be stored. All requests regarding patient personal data must be made in writing to the Information Rights Team within the Information Governance department as outlined in the Subject Access Procedures. The Data Protection Act 1998 states that the data subject's request must be dealt with by the Data Controller within 40 calendar days.

Health bodies can charge a non-refundable fee of a maximum of £10 for this service. A record of all such requests and payments must be maintained.

Anyone who makes a request for access should be given an information leaflet explaining the health body's CCTV procedure. Cumbria Partnership Trust's CCTV information leaflet is reproduced as Appendix 4.

Section 10 of the Data Protection Act 1998 allows an individual the right to prevent processing likely to cause unwanted damage or distress. Any requests of this nature must be dealt with in accordance with the Data Protection Act Policy. A written response must be sent to the data subject within 21 days of receipt of the request, confirming whether images are held and including details for arranging a viewing, if that is appropriate.

When facilitating a request from a data subject to access their own image, any information which would enable the identification of third parties that is held under a duty of confidence must be either removed or obscured. If this cannot be reasonably achieved, access may be

denied. NB – when considering 'subject access requests' only images which clearly identify the subject need be disclosed to them, i.e. the image size should not be less than 120% of screen height.

7.11.3 Freedom of Information

Section 40 of the FOIA and section 38 of the FOISA contain a two-part exemption relating to information about individuals. If a request for CCTV footage is received then the Trust Freedom of Information policy should be adhered to, POL/002/003 refers.

If the request is to view their own image, it should be treated as a data protection subject access request as explained above.

In practical terms, if individuals are capable of being identified from the relevant CCTV images, then it is personal information about the individual concerned. It is unlikely that this information can be disclosed in response to an FOI request as the requester could potentially use the images for any purpose and the individual concerned is unlikely to expect this. This may therefore be unfair processing in contravention of the Data Protection Act (DPA).

7.11.4 Third Party Requests

Images will not be provided to third parties with the exception of law enforcement bodies.

7.11.5 Security Industry Authority License

If the CCTV system covers a public space, consideration must be given to possible licensing requirements imposed by the Security Industry Authority. Under the provisions of the Private Security Industry Act 2001, it is a criminal offence for staff to be contracted as public space surveillance CCTV operators in England, Wales and Scotland without an SIA licence. Any CCTV system that is re-sited and may incorporate a public space not previously covered, advice must be sought from the LSMS or Head of Information.

7.12 Quality of Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. It is therefore essential that suitable equipment is installed appropriate to the conditions/environment in which it is to be used, e.g. the use of infra-red equipment may be necessary in poorly lit areas.

Upon installation, an initial check should be undertaken to ensure that the equipment performs properly.

7.13 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.

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 Head of Information Governance and where necessary advice should be sought from the LSMS. 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.

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.

7.14 Law Enforcement Agencies

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.

7.15 Retention and Disposal of Images

Images should not be retained for longer than is necessary and not longer than 31 days unless an incident occurred and the images are required for evidential purpose.

Once the retention period has expired the images should be removed and erased.

Video should not be kept longer than necessary unless required, for example, as evidence in legal proceedings. If the tapes automatically record information such as location of the

camera and the date and time the picture was taken, it is important to ensure that this information is and remains accurate. A local documented procedure for ensuring the accuracy of this information must be maintained.

All authorised staff with access to images should be trained.

A retention time of 31 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.

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 Information Governance can advise further on this issue.

7.16 Dissemination and Implementation

This document will be circulated to all managers who will be required to cascade the information to members of their teams and to confirm receipt of the procedure and destruction of previous procedures/policies which this supersedes. It will be available to all staff via the Trust intranet. Managers will ensure that all staff are briefed on its contents and on what it means for them.

8. Training

Training will be provided by the Professional Head of Estates and/or the LSMS to key operational staff with responsibility for the local implementation of this policy.

9. Monitoring Compliance with this Policy

The table below outlines the Trusts' monitoring arrangements for this policy/document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect of compliance or effectiveness being monitored	Monitoring Method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
Records of CCTV installations contain all relevant information	Review of CCTV records	The Head of Estates	Annual	Corporate Fire Health Safety and Security	Head of Estates
Systems Level Security Policy (SLSP)	Review of SLSP	The Head of Estates	Annual	Corporate Fire Health Safety and Security	Head of Estates

10. References / Bibliography

Data Protection Act 1998.
European Convention on Human Rights
Freedom of Information Act 2000
Freedom of Information (Scotland) Act 2002
Health and Safety (Display Screen Equipment) Regulations 1992
Human Rights Act 1998.
In the Picture: a data protection code of practice for surveillance cameras and personal information
Information Commissioners Office – Subject Access Request Code of Practice
Mental Health Act 1983
NHS Protect Security Management Service, Security Manual – Section 3.5 – Closed Circuit Television (CCTV).
Police and Criminal Evidence Act 1984
Private Security Industry Act 2001
Public Order Act 1986
Regulation of Investigatory Powers Act 2000

11. Related Trust Policy / Procedures

POL/002/018 Data Protection Act Policy
POL/002/002 Dealing with Complaints and Comments Policy
POL/002/003 Freedom of Information Act Policy
POL/002/19 Health and Safety Policy
POL/002/021 Policy on Safe use of Display Screen Equipment
POL/001/008 Prevention and Management of Violence and Aggression (PMVA)

POL/002/018/01 Procedure for processing Subject Access Requests (access to their personal data)
POL/0002/12 Risk and Safety Strategy & Policy
POL/002/015 Security Policy

Appendix 1 – ICO Registration

Data Protection Register - Entry Details

Registration Number: Z8703662

Date Registered: 06 August 2004 **Registration Expires:** 05 August 2016

Data Controller: CUMBRIA PARTNERSHIP NHS FOUNDATION TRUST

Address:

MAGLONA HOUSE
UNIT 68 KINGSTOWN BROADWAY
CARLISLE
CA3 0HA

This data controller states that it is a public authority under the Freedom of Information Act 2000 or a Scottish public authority under the Freedom of Information (Scotland) Act 2002

This register entry describes, in very general terms, the personal data being processed by:

CUMBRIA PARTNERSHIP NHS FOUNDATION TRUST

Nature of work - NHS Trust/Health Authority

Appendix 2 – CCTV Checklist

This CCTV system and the images produced by it are controlled by …….. who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998)1.

We (……) have considered the need for using CCTV and have decided it is required for the prevention and detection of crime and for protecting the safety of customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

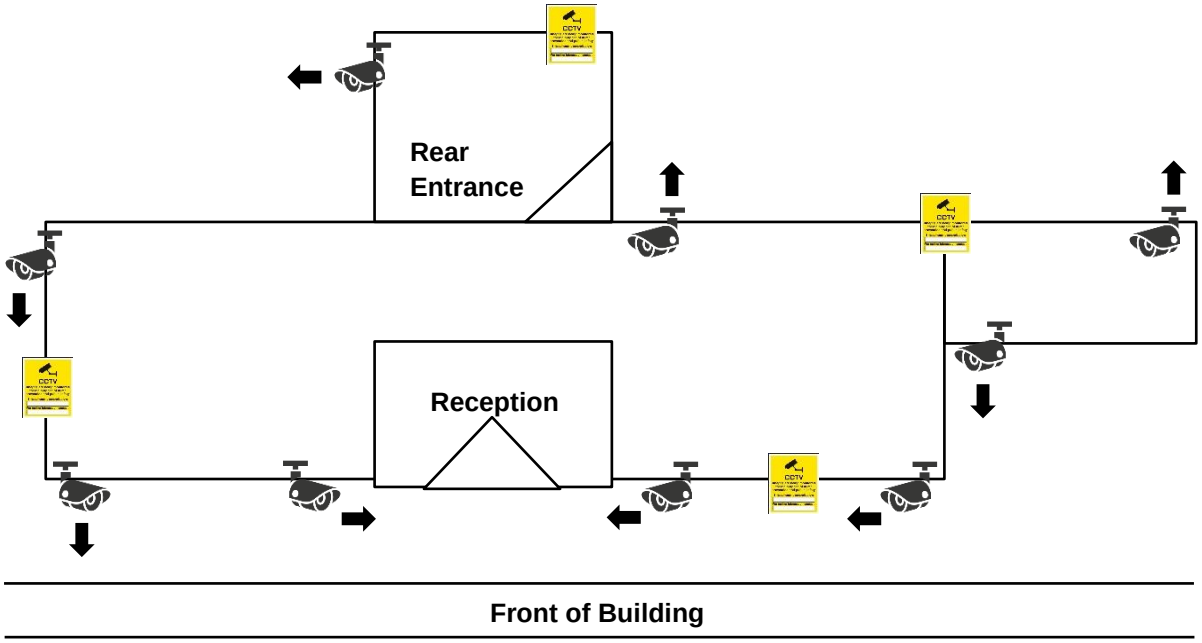
	Checked (Date)	**By**	**Date of next review**
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
The problem we are trying to address has been clearly defined and installing cameras is the best solution. This decision should be reviewed on a regular basis.			
A system has been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			

The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The potential impact on individuals' privacy has been identified and taken into account in the use of the system.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made. Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Please keep this checklist in a safe place until the date of the next review.

Appendix 3 – Location of CCTV Cameras and Signage

* Example Only



Key

= Sign **= Camera**

CCTV Signs

The Data Protection Act 1998 states we have a duty to let people know that they are in an area where CCTV cameras operate, and that signs should:-

- Be of appropriate size, clearly visible and readable (at least A5 size)
- Contain details of the organisation operating the system (unless this is obvious, as it will be in our, the Trust's, case)
- State the purpose for using CCTV and who to contact about the scheme.

An example of CCTV signage to be used:

Appendix 4 – Cumbria Partnership NHS Foundation Trust Closed Circuit *(CCTV) Systems Information Leaflet*

The processing of closed circuit television (CCTV) images is governed by the Data Protection Act 1998. The Information Commissioner has issued a Code of Practice under this Act relating to the use of CCTV systems. All CCTV operators employed by Cumbria Partnership NHS Foundation Trust must comply with the Act and Code of Practice.

Cumbria Partnership NHS Foundation Trust has installed a CCTV system within a number of its premises...

CCTV systems will not be used for any purpose other than that registered with the Information Commissioners Office. Images will not be retained for longer than necessary and will be removed or erased after this period has expired.

Images will not be disclosed to third parties unless the provisions of section 29(3) of the Data Protection Act 1998 are met. Such circumstances may include:-

- The investigation of crime
- The apprehension or prosecution of offenders
- A requirement for disclosure by or under an enactment
- A requirement for disclosure by rule of law or by order of the court
- A requirement for disclosure in connection with legal proceedings (including prospective legal proceedings)
- Disclosure is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

If you wish to make a complaint about the operation of Cumbria Partnership NHS Foundation Trust's CCTV systems please contact:-

Complaints Manager,
Cumbria Partnership Foundation NHS Trust,
Maglona House
Kingstown Broadway
Carlisle
Cumbria
CA3 0HA