NHS
Mersey Care
NHS Foundation Trust
Community and Mental Health Services

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

CCTV POLICY

Policy Number:	**SA18**
Scope of this Document:	**All Staff**
Recommending Committee:	**Health & Safety Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**November 2018**
Next Review Date (by):	**October 2020**
Version Number:	**2018 – Version 5.1**
Lead Executive Director:	**Executive Director of Communications and Corporate Governance**
Lead Author(s):	**Local Security Management Specialist**

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

2018 – Version 5.1

Striving for Perfect Care for the People We Serve

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

CCTV POLICY

Further information about this document:

Document name	**SA18 - CCTV POLICY**
Document summary	**The purpose of this policy is to ensure that the use of Closed Circuit Television (CCTV) adheres to the principles of the Data Protection Act 1998, The General Data Protection Regulations 2018, Human Rights Act 1998, and other relevant legislation. That the good practice set out in the Information Commissioner's CCTV Code of Practice is followed, where appropriate and that any CCTV system is not abused or misused and that CCTV is correctly and efficiently installed and operated.**
Author(s) Contact(s) for further information about this document	**Joe Murray** **Safety Advisor / Local Security Management Specialist (LSMS)** **Telephone: 01254 821559**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Foundation Trust** **V7 Building** **Kings Business Park** **Prescot** **Merseyside** **L34 1PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	**IT14 Data Protection Act Policy** **IT10 Confidentiality & Information Sharing Policy** **SA03 Reporting and Management of Adverse Incidents Policy** **IT12 Information Governance Policy** **Information Commissioner's Office CCTV Code of Practice** **All relevant legislation and guidance referred to within**
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

		Version History:
Here detail the stage of document, e.g., Consultation Draft, Version 1	Presented to the Health & Safety Committee for Approval	8.12.2016
Version 2	Presented to Policy Group	20/12/2016
Version 3		09/01/2017
Version 4	Ratified by Executive Committee	20/07/2017
Version 5	Presented to Policy Group / Ratified by Executive Committee	Oct / Nov 2018

SUPPORTING STATEMENTS

This document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / adult;
- knowing how to deal with a disclosure or allegation of child / adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child / vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
- Ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy / maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

1. PURPOSE AND RATIONALE

1.1. The purpose of this policy is to ensure:

(a) that the use of Closed Circuit Television (CCTV) adheres to the principles of the Data Protection Act 1998, the General Data Protection Regulations, Human Rights Act 1998, and other relevant legislation;

(b) that the good practice set out in the Information Commissioner's CCTV Code of Practice is followed, where appropriate;

(c) that any CCTV system is not abused or misused;

(d) that CCTV is correctly and efficiently installed and operated.

1.2. The overall purpose of CCTV schemes is to maintain the safety and security of Mersey Care NHSFT's staff, service users / carers (particularly those who are entering and leaving the trust premises during the hours of darkness), other individuals who may visit trust premises from time to time and to protect trust premises from criminal activities.

1.3. It is the intention to restrict the view of the camera to ensure that they do not view areas that are not of interest and are not intended to be used for surveillance, or to view private property by utilising the CCTV program to mask off these areas.

1.4. They will also, on occasions, following risk assessment, be used to enhance the security of service users within in-patient areas, monitoring access to bathroom and bed areas. The particular purpose of all schemes, unless specifically identified as directed monitoring (Section 9 refers) are in accordance with the following purposes:

a) to assist in the prevention and detection of crime against both persons and property;

b) to facilitate the identification, apprehension and prosecution of offenders in relation to crime;

c) to protect the health and safety of Mersey Care NHSFT employees, service users, patients and other visitors;

d) to ensure the security of property belonging to Mersey Care NHSFT and employees and visitors to the trust.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1. Prevention or detection of a crime or disorder on Mersey Care NHSFT property.

2.2. Apprehension and prosecution of offenders (including use of images in criminal proceedings).

2.3. To protect trust property and assets.

2.4. To enhance the feelings of security provided to staff, service users and carers.

3. SCOPE

3.1. The policy is binding on all employees of Mersey Care NHS Foundation Trust (Mersey Care NHSFT) and applies also to other persons who may, from time to time, and for whatever purpose, be present on any of its premises. Member of the public/Visitors are aware of the CCTV via the CCTV signage located on site at various locations and also all Contractors are made aware of the CCTV policy via the Tool Box talk.

3.2. The direct management of external CCTV cameras on sites that Mersey Care NHSFT does not manage, but uses accommodation on, will be the responsibility of the person operating such CCTV systems, not Mersey Care NHSFT. Mersey Care NHSFT is only responsible for CCTV systems in respect of which it is the data controller for the purposes of the Data Protection Act 1998 and the General Data Protection Regulations 2018 (GDPR).

4. DUTIES

4.1. All cameras, monitors and data collection and retention processes are maintained operationally by named individual staff on each respective trust-owned site (see Appendix 1) and further maintained by third party provider organisation's under separate maintenance contract to the Trust in accordance with this policy. The Local Security Management Specialists will monitor the use of all CCTV, undertake regular audits to ensure compliance with relevant legislation and guidance and provide advice and guidance on their use.

4.2. It is the responsibility of Mersey Care NHSFT, as overall owner of all CCTV schemes on Trust sites:

a) to ensure compliance with this policy;

b) to ensure that the operating procedures for all schemes are complied with at all times;

c) to ensure that the purposes and objectives of all schemes are not exceeded;

d) to notify all persons on the Trust property where CCTV is installed and that a CCTV scheme is in operation;

e) to facilitate formal subject access requests of any images captured under the terms of the Data Protection Act 1998 & the General Data Protection Regulations;

f) to provide copies of this policy when required to do so;

g) to ensure that all CCTV schemes have appropriate signage to inform people entering and leaving buildings / car parking that CCTV is in operation;

h) to ensure CCTV screens cannot be seen by individuals who are not authorised to do so.

4.3. **Security Management Director**

4.3.1. The lead Executive Director for this policy (Executive Director of Communications and Corporate Governance) has strategic responsibility for:

a) ensuring that there is a consistent and co-ordinated approach to health and safety throughout the trust;

b) bringing the policy to the attention of all trust staff;

c) advising the Chief Executive of any health and safety matters that compromise the effectiveness of the organisational structure, procedures, or systems.

4.4. **Head of Health, Safety and Security**

4.4.1. With the exception of High Secure Services, the Head of Health and Safety (H&S) is responsible for all CCTV systems which includes the following requirements

- Ensuring that a system is in place for the annual testing and inspection of CCTV's systems
- Developing CCTV assignment instructions with the CCTV contractor
- Managing the review and extraction of CCTV images in line with data protection
- Ensuring that CCTV systems are included in the annual report

4.5. **Caldicott Guardian**

4.5.1. Each NHS Trust and Board has an appointed Caldicott Guardian which in the case of Mersey Care NHSFT is the Medical Director. The Caldicott Guardian has a strategic role for the management of patient information. The Guardian's key responsibilities are to oversee how staff use personal health information and ensure that service users' rights to confidentiality are respected.

4.6. **Data Protection Officer**

4.6.1. The Data Protection Officer is the title given to the person with the legal obligations for compliance in respect of the handling of personal data, and faces two obligations in relation to the personal data they hold.

4.6.2. Firstly, a data controller is required to comply with the eight principles of good information handling (the Data Protection Principles), and secondly to let the Information Commissioner know certain details about themselves including the types of information held and the purposes for which they process personal data. All initial correspondence will go to the Head of Health and Safety & Security and the Data Protection Officer (DPO)

4.7. **Local Security Management Specialist (LSMS)**

4.7.1. A nationally accredited post that has responsibility for all security issues within an NHS Trust. The Local Security Management Specialist should have oversight of the output specification and procedures supporting the operational use of CCTV in a health body to ensure compliance with all relevant guidance and provide assurance to Security Management Director (SMD), or other director with legal responsibility for CCTV, that these requirements are being met.

4.7.2. The Local Security Management Specialist should lead on the development of an Operational Requirement (OR) for existing CCTV as well as any new or replacement installations. There should be due regard to the appropriateness of this technology in a healthcare setting - informed by risk assessments and crime prevention surveys - and the need to support it with effective policies on its use

4.7.3. The Local Security Management Specialist, in conjunction with estates and facilities leads, should also ensure that the CCTV system is properly maintained. Requirements and procedures for system maintenance should be considered as an essential element in the design and procurement of the system.

4.8. **Divisional CCTV Manager**

4.8.1. Each division must nominate a single person from the Senior Management Team who has overall responsibility for all CCTV across the division. All requests for viewing images must be authorized by this person (see Appendix 4 & 5). Once authorised this record must be retained three years for audit purposes. Any footage that has been retrieved and found not to be on any evidential use must be deleted.

4.9. **Scheme Manager**

4.9.1. The Scheme Manager is defined as a Service Manager who is responsible on a day-to-day basis for the legal and effective use of a CCTV Scheme.

5. PROCESS

5.1. No CCTV scheme should be initiated, installed, moved or replaced without prior approval by the Caldicott Guardian, or someone delegated to approve such schemes. The Data Protection Officer and the Head of Health and Safety/Security must also be informed.

5.2. All schemes will be monitored and managed using the following procedures and must be formally approved (as above) prior to any installation:

5.2.1. Local Security Management Specialists will assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment and carry out a privacy impact assessment. The assessment process must establish:

a) that there are clearly defined and specific purpose of the CCTV scheme,

b) that the use of CCTV, in the manner proposed, complies with relevant legislation and guidance and is a justified, necessary and proportionate means of achieving such purposes,

c) that the scheme otherwise complies with the requirements of this policy, the assessment process and the reasons for the installation of the scheme will be clearly documented;

d) This information must be held at a central point allowing full access to the Local Security Management Specialists covering the area(s)

5.3. assessment / findings will be shared with the Division involved. Once agreement gained, log with the Information Governance Committee;

5.4. the purpose of the scheme will be documented in accordance with relevant legislation and guidance;

5.5. any new schemes will be checked against the Trust's current notification that is held by the Information Commissioner;

5.6. the person(s) or organisation(s) that are responsible for ensuring the day-to-day compliance with the operational requirements of such schemes and this policy will be documented;

5.7. where an external provider is to be used for any aspect of the scheme, an SLA will be entered into with that provider which specifies the responsibilities of the parties and provides explicit guarantees as to compliance with relevant legislation and guidance. In particular, it should make clear how the information will be used and kept secure;

5.8. each CCTV system will have an accountable 'Scheme Manager' who is responsible on a day-to-day basis for the appropriateness of its use. This will generally be the senior manager of the unit / area concerned;

5.9. the Local Security Management Specialist will liaise bi-annually with all external providers of CCTV Schemes in order to monitor the adherence to the agreed SLA and all relevant legislation and guidance.

5.10. **Principles**

5.10.1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

5.10.2. The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

5.10.3. There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

5.10.4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5.10.5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

5.10.6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

5.10.7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

5.10.8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

5.10.9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use. All requests to access CCTV images must be authorised by the Head of Health Safety Fire and Security.

5.10.10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

5.10.11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

5.10.12. Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

5.11.

5.12.

5.13. **Data Protection Legislation**

5.13.1. Mersey Care NHSFT Data Protection Officer will identify and include in all its schemes within the annual 'Notification' process required by the Data Protection Act 1998, and the General Data Protection Regulations 2018 (GDPR).

5.13.2. All schemes will operate in accordance with the guidelines set out in the 'CCTV Code of Practice' and additional guidance published by the Information Commissioner, a copy of which is available from the Data Protection Officer or direct from the Information Commissioner's website: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

5.13.3. The Trust must adhere to the following guidelines, to conform to the Data Protection Act 1998 and the General Data Protection Regulations 2018 (GDPR).and CCTV Code of Practice:

a) Site / Services Managers operating such schemes within premises they manage will be responsible for overseeing that monitoring of all images are done so in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with the written operational procedures (see Appendix 2);

b) cameras will not be hidden from view and appropriate steps must be taken, eg by signing and displaying posters, to inform the public of the presence of the system and its ownership at all times;

c) to ensure privacy the cameras are fixed and focused only upon Mersey Care NHSFT property, which must be demonstrable upon specific request;

d) images from the cameras are appropriately recorded in accordance with existing operational procedures (see Appendix 2);

e) there is no sound recording undertaken from any part of the system.

5.12 The General Data Protection Regulations (GDPR) 2018:

5.12.1 Due regard will be given to the data protection principles contained in Article 5 of the GDPR which provide that personal data shall:

a) processed lawfully, fairly and in a transparent manner;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and , where necessary, kept up to date;

e) kept in a form which permits identification of the data subjects for no longer than necessary for the purposes for which the personal data are processed;

f) and processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.12.2 The above guidelines are not an exhaustive list of what must be done to comply with the CCTV Code of Practice. Those involved in the implementation, operation or management of CCTV schemes will need to be familiar with the requirements of the Data Protection Act 1998, the CCTV Code of Practice and other relevant legislation and guidance and the General Data Protection Regulations (GDPR).

5.13 **Covert Surveillance**

5.13.1 CCTV schemes established under this policy are overt – people must be made aware that a CCTV scheme is operation and it may only be used for clearly defined and specified purposes.

5.13.2 The targeted, deliberate and covert monitoring or observation of specific persons, including their movements, conversations, activities or communications, is likely to amount to directed or intrusive surveillance for the purposes of the Regulation of Investigatory Powers Act 2000. This Act provides that such covert surveillance can only be authorised and carried out by specified authorities (e.g., the police). Mersey Care NHSFT may not lawfully carry out covert surveillance itself.

5.13.3 In exceptional circumstances, a specified authority that is lawfully able to authorise covert surveillance under the Act (e.g. the police) may request the Trust's assistance in carrying out such surveillance for the purposes of a specific investigation. Such activity will only be permitted with approval of the Chief Executive, having satisfied him or herself that is lawful and appropriate carry out such activity.

5.14 **Installation**

5.14.1 The installation of all schemes must be in accordance with requirements and should remain appropriate to its original identified and documented business purpose in accordance with this policy. An installation process must be adopted in accordance with the checklist outlined in Appendix 3. The checklist and other documents will be held by the Scheme Manager locally and centrally by the Local Security Management Specialist.

5.14.2 When consideration is being given to the use of CCTV, staff must identify the rationale for its installation. These should typically include:

a) prevention of crime;

b) detection of crime;

c) protecting the health and safety of employees, service users and visitors.

5.14.3 It is important that a clear rationale is developed and that potential breaches of confidentiality are considered. It has to be recognised that CCTV has limited efficacy if used inappropriately and can, in some instances, create distress and anxiety in certain individuals. Indiscriminate usage must not occur and will be prevented by close liaison between the Local Security Management Specialist, Clinical Staff, Data Protection Officer and the Estates Department prior to installation by ensuring secure passwords to access DVR/NVR servers or web accessed Systems

5.14.4 During the planning process, alternatives to CCTV usage (e.g., signage, lighting, alarms etc.) should be considered as well as supportive measures such as controlled access to buildings.

5.15 Subject Access

5.15.1 Images of individuals captured by CCTV cameras constitute as their personal data. Under the Data Protection Act 1998, and the General Data Protection Regulations (GDPR). Individuals have the right to obtain copies of their personal data and a description of such data, the purposes for which it is being processed and the recipients (or classes of recipients) to whom it may be disclosed.

5.15.2 A valid request must be made in writing to the Head of Health Safety Fire and Security, however, it does not need to refer to the Data Protection Act 1998 and can be made by any employee or officer of the trust. Therefore, any written request by an individual for CCTV images of him or herself should be treated as a subject access request and followed in accordance with the Trust's Data Protection Act Policy and the General Data Protection Regulations (GDPR).

5.15.3 Only the Data Protection Officer or the Head of Health and Safety/Security, in their absence, the Local Security Management Specialist, in response to a formal request from the data subject, will permit subject access to the images monitored by the system either in hard copy format or by informal viewing. In instances where no recorded images are retained (instantaneous viewing only) data subjects will be informed that the system produces no recordable images and that subject access in these particular instances can only be granted for the purposes of determining the extent of the CCTV monitoring range.

5.15.4 Individuals or their authorised representative wishing to access images from the system or formal subject access requests specifically relating to CCTV must contact the Mersey Care NHSFT's Data Protection Officer. The Data Protection Officer / Local Security Management Specialist will complete the 'Access Log' (see Appendix 4 & 5) and file for a period of three years for the Police & Public/Staff requests.

5.16 Procedures for Processing Subject Access Requests

5.16.1 Data subjects who wish to access Mersey Care NHSFT's information recorded on CCTV systems should be advised to contact the Trust's Data Protection Officer for details about making a subject access request and asked to state the nature of their

relationship with the trust (for example employee, former employee, service user, visitor, contractor).

5.16.2 Any member of staff receiving a subject access request must forward it immediately to the Data Protection Officer to ensure that it is complied with in accordance with statutory deadlines and the Data Protection Act Policy.

5.16.3 Judgments about disclosure of CCTV images (whether under subject access or otherwise) should be made by the trust. The trust has discretion to refuse any request for information unless there is an overriding legal obligation, such as a court order or valid subject access request. The privacy of third parties who are included in CCTV images should be protected by following the procedures set out in the Operational Procedures for the Control and Use of CCTV (Appendix 2).

5.17 **Breaches of this Policy**

5.17.1 Mersey Care NHSFT will investigate any breaches of this policy, using appropriate mechanisms that may include the Adverse Incident Policy or Disciplinary procedure.

5.17.2 A major purpose of this scheme is to safeguard the health and safety of staff, service users and visitors (Section 6 refers). It should be noted that intentional or reckless interference with any part of any monitoring equipment, including cameras / monitor / back-up media, may be a criminal offence and will be investigated by the Trust.

5.18 **Complaints Procedure**

5.18.1 Grievances and complaints regarding the operation of Mersey Care NHSFT's CCTV system may be progressed through the Data Protection Officer or grievance procedures.

5.19 **Related Policies & Codes of Practice**

5.19.1 Other related policies:

a) Data Protection Act Policy (Policy Reference Number: IT14)

b) Confidentiality & Information Sharing Policy (Policy Reference Number: IT10)

c) Information Governance Policy (Policy Reference Number: IT12)

d) Reporting, management and review of adverse incidents (Policy Reference Number: SA03)

e) Information Commissioner's Office CCTV Code of Practice (Revised 2015)

f) The General Data Protection Regulation (2017 –May 2018)

g) Grievance Procedures (HR 02)

6 CONSULTATION

6.1 This Policy has been developed by the Information and Governance Manager and Head of Health, Safety & Security. As part of its development the trust has involved each division that operates CCTV and the Information Governance Committee.

7 TRAINING

7.1 Guidance in the requirements of the law on Data Protection will be given to staff that are required to manage and work with the CCTV systems.

7.2 Staff will be fully briefed and trained in respect of all functions; operational and administrative, relating to CCTV control operation, by the installer of the system or via the Trust Local Security Management Specialist.

7.3 Training by camera installers will also be provided as appropriate to authorised staff

8 MONITORING

8.1 This policy, its operation and the operation of Mersey Care NHSFT's CCTV schemes will be reviewed annually by the trust's nominated Local Security Management Specialist providing an annual report to the Information Governance Committee.

Equality and Human Rights Analysis

Title: CCTV Policy SA18
Area covered: CCTV

What are the intended outcomes of this work? (a) to ensure compliance with the statutory, common law, and trust minimum performance standards; (b) to eliminate or implement appropriate control measures arising out the trust's work activities to reduce identified risk to as low as is reasonably practicable.
Who will be affected? Applies to all activities and functions undertaken by, or on behalf of, the trust and applies to all trust employees and anybody who is or may be impacted upon by work activities of the trust.

Evidence
What evidence have you considered? Information Commissioners Office Approved Code of Practice
Disability (including learning disability) Indirectly due to no reference to 3rd party support in writing for requests under Data Protection Act
Sex No significant issues
Race Standard CCTV identifying signs
Age No significant issues
Gender reassignment (including transgender) No significant issues
Sexual orientation No significant issues
Religion or belief No significant issues
Pregnancy and maternity No significant issues
Carers No significant issues
Other identified groups No significant issues
Cross Cutting **No significant issues**

Human Rights	**Is there an impact?**

	How this right could be protected?
Right to life (Article 2)	Supportive of HRBA.
Right of freedom from inhuman and degrading treatment (Article 3)	Supportive of HRBA.
Right to liberty (Article 5)	Supportive of HRBA.
Right to a fair trial (Article 6)	Supportive of HRBA.
Right to private and family life (Article 8)	Supportive of HRBA.
Right of freedom of religion or belief (Article 9)	Supportive of HRBA.
Right to freedom of expression Note: this does not include insulting language such as racism (Article 10)	Supportive of HRBA.
Right freedom from discrimination (Article 14)	Supportive of HRBA.

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*

Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010*
Eliminate discrimination, harassment and victimisation *Where appropriate the policy is supportive*
Advance equality of opportunity *Where appropriate the policy is supportive*
Promote good relations between groups *Where appropriate the policy is supportive*
What is the overall impact?

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development / change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified*
- *Arrangements for continued engagement of stakeholders*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives*

For the record

Name of persons who carried out this assessment:
1. Kate Greenwood, Jacquie Ruddick, Gina Kelly: 19.10.11
2. Reviewed Tony Crumpton/George Shield: 13/5/2015
3. Reviewed and transferred to new template by Tony Crumpton/George Shield: 01/11/16
4. Reviewed Joe Murray/Dave Berry 16/05/2017

Date assessment completed:
16/05/17

Name of responsible Director:
Medical Director

Date assessment was signed:

Action plan template

This part of the template is to help you develop your action plan. You might want to change the categories in the first column to reflect the actions needed for your policy.

Category	Actions	Target date	Person responsible and their area of responsibility
Monitoring			
Engagement			
Increasing accessibility			

Appendix 1

CCTV SCHEMES CURRENTLY IN OPERATION

Scheme Ref No	Location	Building(s)	No of Recordable Cameras	No of Viewing only Cameras	Scheme Manager	Date Scheme Approved	Operational Responsible Officer(s)	3rd Party Maintenance Contractor

Appendix 2

OPERATIONAL PROCEDURES FOR THE CONTROL AND USE OF CCTV

In accordance with the CCTV Policy all installation and use of CCTV must be conducted in accordance with:

(a) the current CCTV Policy;

(b) the Information Commissioner's CCTV Code of Practice;

(c) the following operational procedures.

Standards

Cameras

(a) cameras must always be operated so that they will only capture the images relevant to the purpose for which the particular scheme has been established and approved; if cameras are capturing areas outside the scheme, theses areas must be masked out

(b) cameras and recording equipment should be properly maintained in accordance with manufacturer's guidance to ensure that clear images are recorded and must be secure using password protection;

(c) cameras should be protected from vandalism in order to ensure that they remain in good working order;

(d) if a camera / equipment is damaged or faulty there should be a separate local procedure for:

  (i) defining the individual(s) responsible for ensuring the camera is fixed,

  (ii) ensuring the camera / equipment is fixed within a specific time period,

  (iii) monitoring and overseeing the quality of the maintenance work;

(e) Cameras should not ever be allowed to view any areas outside of the boundaries of Mersey Care NHSFT properties without prior permission and involvement of the Data Protection Officer.

Operators

(a) all operators of CCTV equipment should be trained in their responsibilities in accordance with Mersey Care NHSFT's policy and this procedure;

(b) all staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

Training

(a) Guidance in the requirements of the law on Data Protection and then General Data Protection Regulations, will be given to staff that are required to manage and work the CCTV systems;

(b) Staff will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation; by Installer of system or via Trust Local Security Management Specialist

(c) Training by camera installers will also be provided as appropriate to authorised staff.

Maintenance

(a) a comprehensive maintenance log will be kept which records all adjustments / alterations / servicing / non-availability of all individual schemes;

(b) any data storage on which images have been recorded will be replaced when it has become apparent that the quality of images has deteriorated;

(c) if the system records location/time/date these will be periodically checked (at least weekly) for accuracy and adjusted accordingly. In the case of alterations due to 'British Summer Time' the system should, as a matter of course, must be checked for accuracy;

(d) in the event that CCTV footage records an incident to be subject to further investigation, or is subject to a data subject access request, a copy of the data media in question shall be provided to the Data Protection Officer for preservation (see 'Access' below');

(e) subject to the above, data will not be retained on the DVR/NVR Server for longer than 31 days from the date of recording;

(f) a review must be undertaken at least annually to continually assess against the stated purpose of the identified scheme, the result of which should be made publicly available should they be requested.

Access

(a) all staff should be made aware of the procedures for granting subject access requests to recorded images or the viewing capabilities of CCTV schemes (as per the CCTV Policy). All such requests (in the first instance) should be notified promptly to the Data Protection Officer in writing; including all Police/Public and staff requests

(b) Criteria for the viewing of data material by non-security related personnel.
At the discretion of the responsible officer individuals may be allowed to view data material:

(i) if they are investigating an untoward incident,

(ii) in the case of a missing patient,

(iii) to identify persons relating to an incident.

Areas which would normally result in permission being refused include:

(i) where the person wishing to view has no legitimate interest or purpose for doing so (for example, they have no connection with the incident or have no management role relating to an incident),

(ii) where the performance of a member of staff not relating to crime, fraud or the investigation of untoward incidents is involved;

(c) access to the recorded images must be restricted to a manager or designated member of staff. All accessing or viewing of recorded images should only occur within a restricted area and other employees should not be allowed to have access to that area or the images when a viewing is taking place;

(d) if images are to be specifically retained for evidential purposes, i.e., following an incident, break-in etc, then these images must be retained on an encrypted Disc/USB in a secure place to which access is controlled;

Requests to access recordings by third parties may be granted in certain circumstances and will arise in a number of ways, including:

(i) requests for a review of recording, in order to trace incidents that have been reported to the Police,

(ii) immediate action relating to live incidents, e.g. immediate pursuit,

(iii) individual police officer seeking to review images

(iv) Local Security Management Specialist seeking to review images

Any such requests must always be justified under relevant legislation and guidance and in accordance with the Data Protection Act Policy & the General Data Protection Regulations 2018. The justification for any disclosure must be recorded in the 'Access Log' (Appendix 4 & 5) and all appropriate documentation used.

If data collection materials are to be handed over to the Police or to Solicitors, in the process of their enquiries, the name and station of that police officer together with a crime incident or reference number and signature must be acquired and retained prior to release **(Appendix 4).** The name, address and telephone number of the Counter Fraud Specialist must also be acquired. If copies are required of the footage on data capture materials, two copies must be made. One copy to be retained by Mersey Care NHSFT and the other given to the Police / Solicitors. The event will be noted in the log and the details and signature of the recipient obtained. In the event of the data capture material being required for evidence, it will be retained for a period recommended by those involved with the case; All evidence provided by Mersey Care NHSFT must be saved on an encrypted Disc or USB.

(e) monitors displaying images from areas in which individuals would have an expectation of privacy must not be viewed by anyone other than an authorised employee of the user of the equipment;

(f) when disclosing CCTV images of individuals, particularly when responding to subject access requests, the Trust must consider whether the identifying features of any of the other individuals in the image need to be obscured. In most cases the privacy intrusion to third party individuals will be minimal and obscuring images will not be required. However, consideration should be given to the nature and context of the footage and decisions should be made on a case-by-case basis by the Data Protection Officer or the Local Security Management Specialist

(g) it may be necessary to contract obscuring out to another organisation. Where this occurs, the Trust must have a written contract with the processor that specifies exactly how the

information is to be used and provides explicit security guarantees. All images must be sent by registered Post & signed for at collection point

Digital CCTV

(a) all digital CCTV systems installed onto Mersey Care NHSFT premises must have the storage capacity to hold a minimum of 31-day footage. In certain circumstances it may be considered appropriate to retain data for a longer period, a full risk assessment must be taken before making a decision for a longer retention period re: the Storage/Memory capability of the DVR/NVR/Server

(b) where digital CCTV is installed all sites must have local access to a DVD recorder/USB ability that is compatible with the system in use;

(c) all sites must hold a stock of blank, write once DVDs and Encrypted USB's;

(d) where there is access to CCTV footage via the network, controls should be put into place so only authorised users are able to use it by password protecting the access to the DVR/Server/Web access point.

Appendix 3
INSTALLATION CHECKLIST

• The Chief Executive or persons with delegated responsibility has approved the installation / alteration to the citation of the camera	•	•
• The purpose for the installation / adjustments have been clearly documented	•	•
• The organisation that is legally responsible for the CCTV scheme has been established	•	•
• Equipment is situated so it can only monitor the intended area of coverage as defined in scheme proposal	•	•
• The cameras are not positioned anywhere that would be considered private e.g., office, toilet	•	•
• Signs are in place showing that CCTV systems are in operations and that the owner of the systems name and contact details are clearly displayed	•	•
• Cameras have been positioned to avoid capturing the images of persons not visiting the premises	•	•
• The recorded images are stored securely with strictly controlled access procedures in place	•	•
• The recorded images are stored for no longer than 31 days	•	•
• A procedure is in place for operational equipment to be checked regularly to ensure it is working order	•	•
• Images will only be made available to law enforcement agencies involved in the prevention and detection of crime, appropriate procedures in place	•	•
• A procedure is in place for dealing with individuals requesting access to CCTV footage (other than law enforcement agencies)	•	•
• An appropriate confidential disposal procedure in place	•	•
• CCTV Installer to carry out an Impact Assessment	•	•

Appendix 4

ACCESS TO VIEW OR COPY – POLICE AND PUBLIC

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

DETAILS TO BE VIEWED

Date:	
Reason:	

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

TO BE COMPLETED IF REMOVED FROM CIRCULATION

Details of what recording medium is handed over. DVD, Flash Drive, etc.:			
Issued To:			
Crime No: (for police only)			
Date Issued:			
Issued By:			
Return Date:			
Authorised by (name): Divisional Manager:			
Signed:		Date:	
I acknowledge receipt of the above (name):			
Signed:		Date:	

Appendix 5 INTERNAL CCTV REQUEST FORM

Date of Request	Location requested	
Request Made By	**Designation**	**Printed Name in Capitals**
Reason for Request		
Name **Signature** **Date/Time**		

Incident Number	**Is the request compliant with Data Protection principles?**
Area incident occurred in	**Specified date/time**
Request Authorised	**Printed Name, Signature, Designation of Authorising Officer (CNM/ LSMS and Date Authorised**

APPENDIX 6
OPERATIONAL PROCEDURE – HIGH SECURE SERVICES

Operational Procedure for the use of Ward Based Closed Circuit Television (CCTV) in High Secure Services

POLICY NUMBER	HSS39
RATIFYING COMMITTEE	High Secure Operations & Performance Committee
DATE RATIFIED	July 2017
NEXT REVIEW DATE	July 2018

STATEMENT:	This operational procedure provides guidance for the safe and appropriate use of ward based CCTV in High Secure Services. The guidance both supports and adheres to the principles, safeguards and requirements of the Mersey Care Trust CCTV Policy (SA18).
ACCOUNTABLE DIRECTOR:	Director of Operations (High Secure Services)
POLICY AUTHOR	Mr M Riding, Deputy Service Manager

1. INTRODUCTION

1.1 These operational procedures provide guidance for the use of closed circuit television (CCTV) in patient areas, in High Secure Services. It supports and adheres to the principles, safeguards and requirements of the Mersey Care NHSFT CCTV Policy (SA18) and the operational procedures for its control and use as outlined in Appendix 2 of the above policy. It also ensures that the use of CCTV adheres to the principles of the Data Protection Act 1998, Human Rights Act 1988 and Regulation of Investigatory Powers Acts 2000.

1.2 The procedure identifies roles and responsibilities for staff in the operation, monitoring, and maintenance of the system, and addresses the requirements for the scheme to be operated fairly, lawfully, and only for the defined purposes set out in Section 6 of the Mersey Care NHSFT CCTV Policy.

1.3 Finally, it is recognised that the introduction of CCTV is merely a complimentary resource to appropriate observation and engagement between staff and patients, and as such its use should not impact upon, nor prove a catalyst for a reduction of staffing levels.

2. PURPOSE OF CCTV

2.1 The purpose of ward based CCTV mirrors that of Section 6 of the Mersey Care NHSFT CCTV Policy, which specifically notes the purpose of all schemes to be:

(a) to assist in the prevention and detection of crime against both persons and property;

(b) to facilitate the identification, apprehension and prosecution of offenders in relation to crime;

(c) protecting the health and safety of employees, service users and visitors;

(d) to ensure the security of property belonging to Mersey Care NHSFT, and to employees and visitors of the trust.

3. KEY OBJECTIVES

3.1 The key objectives of CCTV in patient areas mirrors that of Section 7 of the Mersey Care NHSFT CCTV Policy, which specifically notes the key objectives to be:

(a) the detection, prevention and reduction in the incidence of crime on Mersey Care NHSFT property;

(b) the reduction of incidences of vandalism and criminal damage to the Trust, employees and visitor's property;

(c) to enhance the feelings of security provided to staff, service users and carers.

Whilst the use of CCTV in patient areas within High Secure will provide opportunity for the review of clinical incidents or specific allegations, it is noted that the playback of images looking for generalised evidence of unacceptable patient or staff behaviour is not an appropriate use of the system.

4. LEGAL REQUIREMENTS

4.1 Section 8 of the Mersey Care NHSFT CCTV Policy identifies the requirements for the operation of schemes in accordance with respect to data protection legislation. The use of CCTV in patient areas supports these requirements in that:

(a) managers operating the scheme will be responsible for ensuring that the monitoring of all images are in accordance with the Mersey Care Trust CCTV Policy;

(b) suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with the operational procedures outlined in Appendix 2 of the Mersey Care Trust CCTV Policy;

(c) cameras will not be hidden from view and that signage and posters will be present to inform persons entering patient areas or residing on the ward of the use of CCTV and its ownership;

(d) the cameras will be fixed and focused only upon Mersey Care NHSFT property;

(e) the images will only be recorded in accordance with these operational procedures, which support those identified in Appendix 2 of the Mersey Care Trust CCTV Policy.

There will be no sound recording undertaken by any part of the system.

5. HUMAN RIGHTS ACT 1998

5.1 The Human Rights 1998 places a legal duty on all public authorities not to act in a way that is incompatible with human rights as stated under the European Convention on Human Rights. Mersey Care NHSFT is committed to the Human Rights based approach and seeks to take account of human rights in every thing we do.

5.1 This operational procedure has been developed in line with human rights considerations. Where possible the least restrictive measures have been included which aim to take account of both the human rights of patients, carers and staff.

5.3 Of particular importance is Article 8 of the Human Rights Act 1998. Article 8 is the right to respect for private and family life, home and correspondence. This article protects the individual's right to privacy and prevents a public authority from intruding disproportionately into a person's life.

5.4 Article 8 is a qualified right and therefore there is the need to take this into account. This means that there needs to be consideration of the privacy rights of staff and patients and carers who may be being monitored but there is also the need to balance this out in terms of the legitimate reasons for the introduction of the CCTV, which is to make staff, patients and carers safe. The procedure has attempted to address and take into account the real issue of a private life under Article 8.

5.5 Also of equal consideration is Article 3 which is the right to be free from degrading and inhumane treatment. In terms of patients, the CCTV will be located within communal and public areas within the:

(a) wards such as main access corridors and lounge areas;

(b) rehabilitation services' patient activity areas and social meeting places;

(c) patients' spiritual care area;

(d) primary care areas (e.g. Health Centre).

5.6 However, it will not be used or introduced into private areas such as toilets and bedrooms. This aspect of the procedure attempts to support both Article 3 and Article 8 in being the least restrictive options in relation to the use of CCTV within the high secure service.

5.7 In terms of accessing the DVD recorder and disks and any related aspects this is detailed in the procedure but complies with the Data Protection Act 1998. It is important to note that all current domestic and European data protection law was developed and inspired by Article 8 of the European Convention of Human Rights.

6. TRAINING

6.1 Those staff required to use the CCTV system will receive appropriate training with respects to both operation and administration, depending upon their level of required access. A list of those trained at all levels of operation and administration will be held by the system administrator.

7. AREAS TO BE COVERED

7.1 Only images from:

(a) ward and garden communal areas;

(b) rehabilitation services' patient activity areas and social meeting places;

(c) patients' spiritual care area;

(d) primary care areas (e.g. Health Centre)

will be covered by the system. The interiors of patient toilet, bathroom and bedroom areas will not be monitored. The actual positioning of cameras will be dependent on the patient area.

8. LEVELS OF ACCESS

Levels of access to the system will be in accordance with principles outlined in the trust CCTV Policy and the operational procedures for its control and use, as outlined in Appendix 2 of the above policy.

For the purpose of CCTV in, patient areas in High Secure Services there are to be three levels of access.

8.1 Level One: Basic viewing of live images

All ward based, rehabilitation and health centre staff trained in the use of viewing live images from the system may do so only if they have a legitimate reason for doing so. Legitimate reasons include the observation of areas where specific concern has been highlighted or when suspicious behaviour has been noted. The system is not intended to be viewed constantly, nor for generalised observation of areas where normal patient

or staff activity is noted or expected. This level of access will include the switching of views from one camera to another, or displaying multi-camera views. A staff member with Level One access will not have the ability to playback recorded material.

8.2 Level Two: Viewing of recorded images

The same principles of access above also apply to the viewing of recorded images. This is to say that the viewing of such images is only appropriate where specific concerns or suspicions have been highlighted, or in the clinical review of untoward incidents. The viewing of recorded images should not be used where there is no clinical or security reason or rationale to do so. Access to the viewing of recorded images is restricted to the following groups of staff:

(a) ward managers;

(b) security liaison nurses;

(c) modern matrons;

(d) security managers;

(e) duty managers.

Those staff with Level Two access, are required to ensure that only those with legitimate reasons to view the images do so. They should be vigilant about who else sees the images that they have access to, with the general principle being that those with a higher level of access do not allow others with a lower level of access to view images unless they are involved in the reviewing of an incident or undertaking an investigation. The playback of images should be done in as private a manner as possible in line with data protection principles. Level Two access will be password protected.

8.3 Level Three: Preserving/Making a permanent record of recorded images

The preservation/making of a permanent record of recorded images should only be undertaken on the specific written authority of the system administrator. For the purpose of CCTV in patient areas, in High Secure Services this will be the Deputy Service Manager/HSS Risk Lead, who will subsequently inform the Service Director: Secure Division and the Trust Data Protection Officer of the granted request. The only groups of staff with the level of access to preserve/make a permanent record will be:

(a) ward managers;

(b) rehabilitation team leaders;

(c) security liaisons nurses.

As with Level Two, access at Level Three will be password protected. Permanent copies of images will be burned to DVD. It is the responsibility of the system administrator to ensure that all permanent copies of recordings are held in a central secure location, and are encrypted, with access only given to those according to agreed access levels. The system administrator will ensure that blank one use DVD's are made available to those with Level Three access as required.

9. ACCESSING IMAGES

Individual patients (or their legal representatives), staff or visitors whose images are recorded have a right to view the images of themselves and, unless they agree otherwise, to be provided with a copy of the images.

9.1 Application to view images or to request a permanent copy

Any access to view footage or for a permanent copy by a data subject (or a legal representative acting on their behalf) must be made in writing. If an application is made by a legal representative, this must be accompanied by a signed authority from the data subject providing authorised consent for the legal representative to make this request on their behalf.

Where a request is "*manifestly unfounded or excessive*" a search fee will be charged in accordance with the General Data Protection Regulations.

Any viewing of footage will be facilitated by prior arrangement with the system administrator who will arrange the viewing in a private area. Before a patient is allowed to view CCTV footage or is provided with a permanent copy, this must be agreed by the Responsible Clinician following discussion with the Clinical Team including the Security Liaison Nurse. The Data Protection Officer must also be consulted in the event that the footage in question includes other individuals.

In the event that viewing is approved, a risk management plan must be produced and recorded in the patient's electronic record (PACIS).

Where a Responsible Clinician refuses an application to access CCTV footage this must be for a justifiable reason and clearly documented. The patient has the right to appeal to the Executive Director for Secure Services or the Information Commissioners Office.

9.2 Playback of recorded images by Level Two access users

Whenever Level Two access users playback recorded images they are required to complete a written record, which identifies the reasons for the review of the images and the people who have viewed them. This written record is to be sent to the system administrator on a monthly basis.

9.3 Requests by Investigating Officers to view images or have a permanent copy

An appointed investigating officer may be given access to CCTV images pertinent to the investigation (providing the investigation is associated with the stated purpose of the CCTV scheme and subject to the principles of the Data Protection Act 1998).

Only the images relating to the specific events at the centre of the allegation or incident should be considered during the investigation. All requests for access must be made in writing to the system administrator, who will subsequently authorise a Level Two access user to facilitate the request to view the images, or a Level Three access user to facilitate the making of a permanent copy.

9.4 Requests by staff to view images or have a permanent copy

Should a staff member be subject to a disciplinary investigation, it may be appropriate to grant them or their staff side representatives access to CCTV images pertinent to the investigation (providing the investigation is associated with the stated purpose of the CCTV scheme and in accordance with and subject to the principles of the Data Protection Act 1998). Only the images relating to the specific events at the centre of the allegation or incident will be accessed. All requests for access must be made in writing to the system administrator, who will subsequently authorise a Level Two access user to facilitate the request to view the images, or a Level Three access user to facilitate the making of a permanent copy. The Data Protection Officer must also be consulted in the event that the footage in question includes other individuals.

9.5 Requests by the Police (or Other Third Party Agencies) to access images

Some incidents may constitute criminal acts, e.g. theft or assault, and the CCTV images may be useful in the prosecution of individuals committing such acts. In these circumstances, all necessary co-operation will be given to the police in pursuit of their duties (subject to Section 29 of the Data Protection Act 1998). During the course of criminal investigations, it may be appropriate to permit the police to view images recorded by the system. Such requests should be formally made in writing to the Executive Director for Secure Services. The police may also require a permanent record of the image. The removal of the permanent record outside of High Secure Services will require the prior approval of the Executive Director for Secure Services and will be coordinated by appointed Local Security Management Service Officer.

Once a case has been concluded, the police should return their copy of the data to the Local Security Management Service Officer, who will forward it to the system administrator. A written record of such returns will be kept by the system administrator.

Other third party agencies, e.g. Independent Mental Health Advocates (IMHAs) and Independent Mental Capacity Advocates (IMCAs), may also request to see images, however, they would need authorised consent of the service user, if the service user is capable of giving consent. Any third party requests should be forwarded in writing to the Executive Director for Secure Services.

The justification granting any third party access to images shall be recorded.

9.6 Timescales

All responses to those requesting access to the images should be provided promptly and, in any event, within 40 days in accordance with the Data Protection Act 1998.

9.7 Manipulation of images

All images provided to patients, visitors or staff as a permanent copy will have third-party faces blurred out (i.e. pixelated) to maintain confidentiality. Where a specialised company is hired to ‘blur out’ images, this will be under a contractual arrangement with specific references to confidentiality.

9.8 Decision making

In considering requests for access to images, the Executive Director for Secure Services may be assisted by the High Secure Division Directors, the Data Protection Officer, or other panel of suitable membership and will use the guidance issued by the Information Commissioner. The final decision will be made by the Executive Director for Secure Services unless they exercise their discretion and appoint a nominated deputy to make the decision.

10. DATA STORAGE

The system is designed to store a maximum of 31 days worth of recorded data. Data will be automatically re-written after this time.

All exported CCTV images must be permanently destroyed once they are no longer required, e.g. a prosecution or investigation has been completed. The disposal will take place by breaking the DVD into pieces rendering them unusable and placing them in the confidential waste shredder.

The long term safe-keeping of permanent records can only be authorised by the Deputy Service Manager / HSS Risk Lead. Those discs kept for longer term safe-keeping must be kept secure by the system administrator.

Whilst observations made via the CCTV system may be referenced in the clinical record for a patient, the images themselves are not to be used as part of the clinical record and permanent records of them do not, therefore, form any part of the patient's single healthcare record.

11. SYSTEM ADMINISTRATION

The CCTV System Administrator is the Deputy Service Manager/HSS Risk Lead, who will be responsible for the registering and de-registering of Level Two and Level Three users and keeping an up-to-date record of staff that are registered at all levels. They will ensure that staff are able to use the system competently and are conversant with these operational procedures.

They will ensure the maintenance of an accurate administration system for CCTV in line with standard operating procedures including storing, viewing, copying, issuing permanent records, equipment testing and fault reporting. They will also be responsible for the keeping of all requests to access images.

12. COMPLAINTS

Any complaints about the use of CCTV should be made through the Trust's complaint procedure. Alternatively individuals are entitled to make a complaint direct to the Information Commissioners Office.

13. SYSTEM EVALUATION AND AUDIT

A report will be prepared by the administrator of the CCTV system on an annual basis for the attention of the Secure Governance Board. The report will include summaries of all requests for data, instances of its use, its impact on the level and type of incidents, audit records and a commentary on its effectiveness.

5 PATIENT INFORMATION

A patient information sheet is available and is reproduced with these operational procedures.