Closed Circuit Television (CCTV) Policy (F-002)

Version Number:	2.4
Author (name & job title)	Vickie Shaw, Health & Safety Advisor and Security Lead
Executive Lead (name & job title):	P Beckwith, Director of Finance
Name of approving body:	EMT
Date full policy approved:	26 June 2023
Date Ratified at Trust Board:	*(Version 2.1)* June 2018
Next Full Review date:	June 2026

Minor amendments made prior to full review date above (see appended document control sheet for details)	
Date approved by Lead Director:	*26 June 2023*
Date EMT as approving body notified for information:	*26 June 2023*

Policies should be accessed via the Trust intranet to ensure the current version is used

Contents

1. INTRODUCTION

This policy covers the requirements detailed in the Data Protection Act 2018, General Data Protection Regulation (GDPR), The Protection of Freedoms Act 2012 and the CCTV Code of Practice 2008 and is aimed at the use of CCTV and similar surveillance equipment that monitor and record images from those areas to which the public have largely unrestricted access. In addition, areas which have controlled access will also be monitored by the system in order to assist in the protection of public**,** patients, visitors and staff.

The primary objectives being:

- Prevention and Detection of crime
- Public safety
- Maintenance of the public perception of the Trust

This policy supports the compliance with the Care Quality Commission Regulation 15, Outcome 10 '**Safety and suitability of premises** People that receive care in, work in or visit, should feel safe in their surroundings that promote their wellbeing'.

2. SCOPE

This policy sets out the Trust's approach to the management of Close Circuit Television (CCTV) throughout the organisation and applies to all directly and indirectly employed staff within Humber Teaching NHS Foundation Trust and other persons working within the Trust in line with the Trust's Equal Opportunities Documentation. The policy has relevance for those staff members who have responsibility for using or managing CCTV systems or acting as the Trust's point of contact for enquiries. This document is also relevant to Independent Contractors occupying Trust premises.

3. DEFINITIONS

The Trust is committed to ensuring compliance with legal requirements using them as a minimum standard and seeking to exceed those standards in order to protect staff. The Trust is also committed to ensuring a healthy and safe place in which to work and receive care and treatment.

The Trust aims to balance the rights and responsibilities of people using its services with those of employees, with a clear approach to Security Management.

The intended outcome of this policy is to provide the Trust and staff with the knowledge and skills to effectively reduce and manage the risk from adverse risks in the workplace.

The objectives are to: -

- Maintain and improve working environments to ensure, a safe and secure working environment.
- Identify who is responsible for a CCTV system within the Trust, the remit and scope of their roles.
- State the Trust's commitment to improving working environments to ensure, a safe and secure working environment for service users, staff and visitors.
- Ensure Trust employees are aware of and can access mechanisms to maintain and improve working environments.
- Prevent unfair intrusion into the privacy of members of the public and patients

4. DUTIES AND RESPONSIBILITIES

Trust Board
The Trust Board has overall responsibility for monitoring compliance with and effectiveness of, all Trust policies, and will ensure that effective management systems are in place to achieve high standards of health, safety and welfare. The chief executive is the accountable officer and has overall responsibility for health, safety and security matters and will ensure that this policy is implemented in all directorates and reviewed on a regular basis.

Caldicott Guardian
The Executive Director of Nursing Allied Health & Social Care Professionals has been appointed as the Caldicott Guardian for the Trust and has a strategic role for the management of patient information. The Caldicott Guardian's key responsibility is to ensure that service user's rights to confidentiality are respected.

Security Management Director
The security management director has the lead responsibility for Security Management and delegate's day to day management of CCTV systems to the Local Security Management Specialist.

Directors, General, Service & Line Managers
Directors, general, service and line managers are responsible for managing and ensuring the CCTV systems within their area of responsibility are functioning correctly. They are also responsible for the day-to-day security of their working areas and implementation of Trust security procedures. They are additionally responsible for ensuring all staff report breaches of security, criminal activity, incidents, CCTV systems failure, or suspicions to security services in the area where they work immediately.

Local Security Management Specialist (LSMS)
Local security management specialist has responsibility for helping to ensure that this policy allows the Trust to comply with their legal responsibilities.

The LSMS must be consulted regarding operational requirements for new or replacement CCTV systems and must hold a comprehensive list of CCTV cameras across the Trust and will carry out Subject Access Requests.

The LSMS 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 Codes of Practice.

Head of Information Governance and Legal Services/Data Protection Officer
Is responsible for advising the Security Manager Director on systems and procedures that need to be in place to ensure compliance with regards to the ICO's Code of Practice on CCTV, the Data Protection Act 2018 and the General Data Protection Regulation. The Head of Information Governance will ensure that the notification to the Information Commissioner relating to the use of CCTV equipment on Humber Teaching NHS Foundation Trust premises is maintained.

Site Managers
Site managers are responsible for ensuring that systems and procedures are in place on the site for which they have responsibility to ensure compliance with this policy and the information commissioner's code of practice and report any faults to the Estates Helpdesk.

Employees
Employees have a responsibility to abide by this policy and any decisions arising from the

implementation of it.

Employees of the Trust have responsibility for: -

- Ensuring that effective measures are taken to ensure that the Trust premises and property are maintained in a secure condition.
- Taking steps to safeguard against loss of the Trust property and the property of individuals.
- Taking reasonable steps to ensure security of their own personal possessions – the Trust takes no responsibility for personal possessions except in specific circumstances where personal property is handed to staff for safe keeping.

The Head of Information Governance & Legal is responsible for providing advice on the disclosure of material in response to subject access requests.

5. PROCEDURES RELATING TO THE POLICY

Purpose of CCTV Use within the Trust

Within the Trust, CCTV is used for the following purposes:

- The prevention and detection of crime – National Security
- The prosecution of offenders
- The management of safety and security for staff and the public
- Should there be any breaches of Trust rules, the CCTV may be used in disciplinary action
- Investigate allegations or serious concerns about possible abuse or crime

Within the Children and Adolescent Mental Health Service (CAMHS) recordings of therapy sessions may be undertaken as part of the therapeutic intervention which may be offered to the young people and their families, it may also be used to support research and the supervision of staff as a part of clinical training. Any sessions recorded specifically for the purposes of an approved research study, would have separate consent for recordings being taken as part of the Heath Research Authority (NHS Ethics) approved process. These activities are in compliance with the Trust's Photographing, Video and Audio Recording Procedures with regards to consent and why the footage is being recorded and what the images are being used for. When footage is used for clinical training, it is deleted as soon as practicable after the training is completed.

Siting of Cameras

It is essential that the location of the equipment is carefully considered, because the way in which images are captured must comply with the following standards:

- The equipment should be sited in such a way that it only monitors those spaces which are intended to be covered by the equipment
- If residential areas are not intended to be covered by the CCTV system and they border the Trust's grounds, then the Trust should consult with the resident if images might be recorded. Operators must be aware of the purpose(s) for which the scheme has been established
- Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed
- If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces which are not intended to be covered by the scheme
- If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered.
- Where practicable, systems should be capable of masking neighbouring spaces to prevent inadvertent collateral intrusion.

- The equipment is not to be placed where privacy and dignity of a service user may be compromised. This includes toilet areas, bedrooms or similar.
- Except when specifically authorised, using specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA), cameras will not be directed at an individual, their property, or a specific group of individuals.

Camera Signs
Signs (appendix 3) must be placed so that the public are aware that they are entering a zone which is covered by surveillance equipment. The size of signs will vary according to circumstances, the signs must be clearly visible and legible and contain the following information:

- identity of the person or organisation responsible for the scheme;
- the purposes of the scheme;
- details of whom to contact regarding the scheme (e.g., the phone number of reception/control room where the equipment is used).

Quality of Images
Images produced by the equipment must be of sufficient quality as to enable the identification of persons suspected of committing criminal acts, witnessing such acts or in support of other security issues from recorded images.

The CCTV system should be regularly checked to ensure that the recorded images are of good quality, the date and time of the system checked for accuracy, a check that the cameras are working and the quality of the recorded image is sufficient.

Any problems should be rectified as soon as is practicable by requesting a service engineer through the estate's helpdesk.

Storage and Retention of Images

- Images should not be retained for longer than is necessary, as stated by Data Protection Act 2018 and GDPR. The Trust will retain all images for 30 days unless they relate to a specific incident or investigation. This is a requirement of the Department of Health Code of Practice on record retention.
- Once the retention period has expired all recorded images are automatically re-recorded over. Images retained for evidential purposes are to be stored securely. Further advice relating to the storage of evidential images can be obtained from the Trust Local Security Management Specialist (LSMS).

Storage and retention shall only be used for the purpose defined in this policy. Images/recordings shall not be sold or used for commercial purposes or the provision of entertainment

- All recordings are the property of the Trust
- Where the images are required for evidential purposes in legal or Trust disciplinary proceedings, they can either be stored in a secure password protected area of the hard drive-in separate file or downloaded onto cd-r

Authorised person to download images
During working hours, the LSMS will visit site as soon as appropriate and will view the footage with the manager who made the request. Footage will be downloaded (if appropriate) on to a USB stick and then the images will be saved onto the main Trust server and then actioned accordingly.

During Out of Hours, the Estates on call Manager will contact the installer or the main external maintainer security company to download the footage onto a USB stick. The Estates on call manager will visit site and save the footage from the USB onto the main Trust server and then contact the on call Manager/Director and then act accordingly.

Viewing of Images (Live and Recorded)
CCTV images can only be viewed when necessary. This information is only to be accessed by authorised staff. All other staff must be clear of this area and if the area is the reception area, it should be ensured that it is clear of clients, i.e., closed.

Recorded images should be viewed in a restricted area, such as a designated office.

The monitoring or viewing of images from areas where an individual would have an expectation of privacy should be restricted to fully authorised persons only.

Any viewing of images should be documented on the viewing of CCTV images Form (Appendix 1) and sent to the LSMS.

All images will be downloaded and provided to the LSMS by the system installer/main external maintainer security company upon an official request from the LSMS or Estates on call managers.

Subject Access Requests
An individual may request a copy of any recording that exists of them and will only be granted in line with Trust Access to Health Records policy.
The LSMS has responsibility for the receiving and logging all subject access requests and should deal with all requests. All staff involved in operating the equipment must be able to recognise a request for access. Individuals requesting access (the Data Subjects) should be provided with:

- A request for CCTV Image – Subject access under Data Protection Act 2018 form which indicates the information required to locate the images requested. (Appendix 2)
- This policy, which describes the types of images which are recorded and what purpose they are recorded for.

The LSMS is to ensure that a copy of the request form is received before images are released and that the original form is retained.

If the formal request is received after the 30 day retention schedule the footage will no longer be available.

Access may be denied where such an action would compromise the detection or prevention of crime, the security of the Humber Centre Hospital or where it may impede the apprehension or prosecution of offenders.

Any requests received for the disclosure of CCTV footage under the Freedom of Information Act 2000 will be directed to the Legal and Information Governance Team, where such requests will be considered within the strict guidelines of the Act.

Disclosure, Viewing & the Provision of Copies of Images by the Data Subject
If the individual making the request is unknown to the Trust, a photograph of the individual may be requested to locate the correct image. A written response should be sent to the individual within 21 days of receipt of the request, confirming whether images are held and including details for arranging a viewing, if appropriate. It is a requirement of the Data Protection Act 2018 to provide the information (or refusal notice) to the individual within one calendar month of their original request.

One calendar month is calculated from the day the Trust receives the request (whether it is a working day or not) until the corresponding calendar date in the next month. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, the Trust has until the next working day to respond.

This may be extended by two further months where necessary, considering the complexity and number of requests. An example of a complex request would be where the LSMS determines that the disclosure to the individual would entail disclosing third party images. If third party images are to be disclosed as an incidental part of the recording, then the LSMS should arrange for the images of third parties to be disguised, blurred, redacted or obscured.
Data subject must be informed of any such extension within one month of receipt of the request, together with a reason for the delay.

All requests to view CCTV footage must be reasonable, it would not be reasonable for example for someone to request to view a full 24-hour period consisting of multiple cameras. All decisions on whether data subjects can view CCTV images will be made on their individual merits.

Disclosure, Viewing and the Provision of Copies of Images by Third Parties – Police, Insurance companies (i.e., not the data subject)
The police or other investigatory authority (for example the NMC, GMC or CQC) may request a copy of CCTV for the purposes of investigating an alleged crime or incident which has been reported by a member of staff, patient, family member or member of the public.

All CCTV provided to the police will be in its original unedited format, the police will then assess whether their forensic digital services team need to pixilate third parties.

CCTV images provided to other external agencies may have third parties pixilated unless consent has been gained from the third parties contained within the footage, this decision will be taken in consultation with Information Governance Department.

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, to ensure that the rights of individuals are preserved. Disclosure of the recorded images, whether motion or still images, to third parties should only be made in limited circumstances. Reason(s) for which they may disclose copies of the images are compatible with the registered reason(s) or purpose(s) for which they originally obtained those images.

All requests for images must be directed to the LSMS. The Request for CCTV Image – Subject access request form (Appendix 2) should be provided by the requestor. During out of hours CCTV images can be requested by Estates on call direct to the main external maintainer security organisation. Estates will then inform the LSMS the next working day with all the relevant information relating to the request.

All access by third Parties to the device on which the images are recorded should be documented on the Viewing of CCTV Images Form (Appendix 1).

Access to the data will be given to the police subject to the requirements of any information sharing agreement. Access should be recorded on the form for ‘application for access to CCTV images by authorised agency (police)’ (Appendix 3). Two copies of the images will be made showing the incident(s), one for the third party and one to be retained securely either on site or with the LSMS.

All documentation relating to the management and operation of CCTV together with all subject access request forms must be securely retained for a minimum of 3 years, followed by confidentially destroying. Any images that have been retained for evidential purposes will be retained for the minimum period necessary to serve that purpose which will necessarily need to be decided on a case by case basis.

Use of CCTV Footage for Disciplinary Purposes
Only in the circumstances detailed in this section may CCTV footage be used in proceedings

under disciplinary policy.

In the event that recorded CCTV footage reveals activity that the Trust could not reasonably be expected to ignore, then the relevant CCTV footage may be considered during investigatory stages of the formal disciplinary process, and later used in formal disciplinary hearings, if relevant to the allegations against the employee.

If such CCTV footage is identified it will be presented to the employee in the usual way, pursuant to the disciplinary policy. The employee will not be required to make a data subject access request to view the CCTV footage as part of this procedure. Wherever possible, the employee will be given the opportunity to review the CCTV footage and explain or challenge its content. The employee will also be permitted to make representations regarding the CCTV footage in any disciplinary hearing.

Covert Recording
Covert recording shall not be undertaken, all recording must be overt. Any covert recording (including recordings by patients and visitors) would be considered a breach of this policy and may constitute a criminal offence.

Any use of covert recording must be approved by EMT.

Training
All personnel who are required to operate or manage a CCTV system are to be properly trained on the system equipment they are required to use. These individuals must be competent in producing evidential material from the system for which they are responsible.

The provision of training for non-security personnel should be written into the installation contracts for all future, new and refurbished systems to ensure compliance. Local staff must be trained to conduct routine systems checks in accordance with this policy, including date/time stamp corrections. They should also be trained to produce evidential image discs for the police.

Training on legacy systems should be conducted by the system installer/main external maintainer security company . Due to potential costs, this should be fully researched and risk assessed, based upon historical data and new developments in and around the site which may affect the Trust's exposure, prior to entering any contractual arrangements. Advice should be sought from the LSMS regarding this matter.

6. CONSULTATION

Consultation with Health & Safety Group and the Information Governance Group members, which include Modern Matrons, Human Resources Department, Occupation Health Department, Safety and Information Manager, Head of Estates, Representatives from the Estates Department, Infection Prevention and Control Department, Hotel Services and Information Governance team

7. IMPLEMENTATION AND MONITORING

This policy will be disseminated by the method described in the Document Control Policy.

It is the decision of the author as to whether this policy requires additional financial resource or not:

This policy requires additional financial resources.

The contact point indicated on the displayed signs should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing use of the equipment.

Enquirers should be provided on request with:

- A copy of this policy.
- The complaints procedure to be followed if they have concerns about the use of the system.
- Any complaints arising from the management and operation of CCTV will be dealt with under the Trusts normal complaints procedure.

8. REFERENCE TO ANY SUPPORTING DOCUMENTS

The following items of legislation are relevant to this policy:

- Crime and Disorder Act 1998
- Criminal Justice and Public Order Act 1994
- Criminal Procedure and Investigations Act 1996
- Human Rights Act 1998
- Private Security Industry Act 2001
- Police and Criminal Evidence Act 1984
- Regulation of Investigatory Powers Act 2000
- Data Protection Act 2018
- General Data Protection Regulation (GDPR)

Cameras for use in Mental Health Premises/Hospital Environments
The following External publications have helped inform the development of this policy:

- CCTV Code of Practice, Information Commissioner's Office, January 2008
- CCTV Operational Requirements Manual - Is your CCTV system fit for purpose?
- N Cohen, J Gattuso, K MacLennan-Brown, 2009
- NHS Confidentiality Code of Practice, Dept of Health, Nov 2003

The following internal documents have also been considered when developing this policy:

- The Information commissioner's Code of Practice on CCTV systems available on the web at https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- The Data Protection Act 2018
- The Information Commission's Guide to the General Data Protection Regulation (GDPR)
- British Standards Institute publications BS 7958:1991 'Closed Circuit Television (CCTV) – Management and Operation Code of Practice'
- UK Police Requirements for Digital CCTV Systems.
- CCTV Operational Requirements Manual, Publication No. 55/06, Home Office Scientific Development Branch.

9. RELEVANT TRUST POLICIES/PROCEDURES/ PROTOCOLS/ GUIDELINES

- Information Governance Policy P029
- Physical Security Policy P051
- Risk Management Strategy Policy P071
- Health and Safety Policy P036
- Network Security Policy P118
- Photographing, Video and Audio Recording Procedure

APPENDIX 1 - REQUEST BY THIRD PARTY OR TRUST STAFF TO VIEW CCTV IMAGES FORM

Premises			
Location (ie female corridor, outside office etc)			
Camera number/name – if known			
The date and time	Date	Time from	Time to
Reason for the request (Assault, criminal damage, AWOL)			

To be completed by the H&S Advisor and Estates on call Manager

The name of the operator removing the images for viewing	Scamp Security/TESS/Another
The name of the person(s) viewing the images (If this includes third parties, then the name of the person and the organisation should be included).	
The outcome, if any, of the viewing.	
Location and name of the saved footage	..\..\..\CCTV OOH

Please send completed forms via email to the Health and Safety Advisor & Security Lead during working hours and Estates on call manager out of hours

APPENDIX 2 - REQUEST FOR CCTV IMAGE/DISK

NOTES TO ASSIST IN COMPLETION OF THE FORM

DECLARATION (Note 2)

The person making the application must complete this section.

a) If you are the data subject – tick the first box and sign the authorisation then proceed to section 5.

b) If you are completing this application on behalf of another person, in most instances, we will require their authorisation before we can release the data to you. The data subject whose information is being requested should be asked to complete the 'Authorisation' section of the form. (Section 5)

c) If the data subject is a child i.e., under 16 years of age the application may be made by someone with parental responsibilities, in most cases this means a parent or guardian. If the child can understand the nature of the application, his/her consent should be obtained or alternatively the child may submit an application on their own behalf. Generally, children will be presumed to understand the nature of the application if aged between 12 and 16. However, all cases will be considered individually.

REQUEST FOR CCTV IMAGE/DISK
SUBJECT ACCESS UNDER DATA PROTECTION ACT 2018

You are advised that the making of false or misleading statements in order to obtain access to personal information to which you are not entitled is a criminal offence.

SECTION 1: DATA SUBJECT DETAILS

Please supply a photo to aid in identification:

PHOTO

SURNAME:	**DATE OF BIRTH:**
FORENAME(S):	**GENDER:**
Address: **Postcode:**	**Home Telephone No:** **Work Telephone No:**

Proof of identity

To help establish your identity, your application must be accompanied by TWO official documents that, between them prove your identity and address

Current signed passport	Proof of address
Residence permit issued by the Home office	Recent (within 3 months) utility bill
Current UK photo card driving license	Local authority council tax bill
Birth certificate	Current UK photo care license
HM Forces ID Card	Bank, building society passbook
Adoption Certificate	Current local council rent book
Marriage/civil partnership certificate	Department of Works and Pensions original notification letter
Divorce or annulment papers	Court Order (within 12 months of current date)

SECTION 2: DECLARATION STATEMENT (Note 2)

This section must be signed in the presence of the person who certifies your application.

I declare that the information in this form is correct to the best of my knowledge and that I am entitled to apply for access to personal data referred under the terms of the Data Protection Act 2018.

Please tick appropriate box

I am the person named Signature of Data Subject: Date: **or**	
I am the agent for the person named and I have completed the authorisation section	
I am the parent/guardian of the person who is under 16 years old and has completed the authorisation section	
I have been appointed by the Court to manage the affairs of the person	

SECTION 3: APPLICANT DETAILS - The applicant is the person who is applying on behalf of the data subject to get access to the CCTV footage.

Applicants Name (please print)	
Address to which reply should be sent (if different from over, inc Postcode)	
Signature of Applicant	

SECTION 4: LOCATION - Provide details of the camera location, and the date and time of the footage you would like to see, as well as a general description of the incident

To help us find the information

Date and time of incident	
Place incident occurred	
Brief description of incident	

SECTION 5: AUTHORISATION STATEMENT

I hereby authorise NHS Organisation …… to release CCTV images they may hold relating to me to …… (Enter the name of the person acting on your behalf) to whom I have given consent to act on my behalf.

Signature of Data Subject Date ……

OFFICIAL USE ONLY

Date Request Received			
Date Form sent to Applicant			
Date Form Returned		Date sent to System Administrator	
Certification Checked		Data checked	
		Date completed	

Please return the form to: ALSMS, Mary Seacole Building, Willerby Hill, Beverley Road, Willerby, HU10 6ED

APPENDIX 3 – CCTV IN OPERATION DISPLAY POSTER

APPENDIX 4 - DOCUMENT CONTROL SHEET

This document control sheet, when presented to an approving committee must be completed in full to provide assurance to the approving committee.

Document Type	Policy		
Document Purpose	To ensure compliance with the Information Commissioners Office and the Data Protection Act 2018		
Consultation/ Peer Review:	Date:	Group / Individual	
list in right hand columns consultation groups and dates ->	December 2022	Health & Safety Group	
Approving Committee:	EMT	Date of Approval:	26 June 2023
Ratified at:	Trust Board	Date of Ratification:	
Training Needs Analysis: *(please indicate training required and the timescale for providing assurance to the approving committee that this has been delivered)*	Training requirements for these procedures for management to implement	Financial Resource Impact	This policy requires additional financial resources
Equality Impact Assessment undertaken?	Yes [✓]	No [ ]	N/A [ ] Rationale:
Publication and Dissemination	Intranet [✓]	Internet [ ]	Staff Email [ ]
Master version held by:	Author [✓]	HealthAssure [ ]	
Implementation:	*Describe implementation plans below - to be delivered by the Author:*		
	• Shared within communication email to all staff as per Trust procedures via the Communications Department		
Monitoring and Compliance:	Monitoring and compliance of the policy will be evidenced through the Health & Safety Group and by the Local Security Management Specialist.		

Document Change History:			
Version Number / Name of procedural document this supersedes	*Type of Change i.e. Review / Legislation*	*Date*	*Details of Change and approving group or Executive Lead (if done outside of the formal revision process)*
v2.1	*Legislation*	*June 2018*	*Change to national guidance relating to charges for data requests (section 5.7) and time scales (Section 5.8)*
v2.2	*Additional information added*	*June 2019*	*Included specific paragraphs relating to recording therapeutic sessions for training and research purposes only*
v2.3	*Legislation*	*February 2020*	*Reference updated to revised Data Protection legislation*
v2.4	*Review*	*June 2023*	*Addition of poster, removal of disclosure to the media, further details on subject access requests. Approved at EMT (26 June 2023).*

APPENDIX 5 - EQUALITY IMPACT ASSESSMENT

For strategies, policies, procedures, processes, guidelines, protocols, tenders, services

1. **Document or Process or Service Name:** CCTV Policy
2. **EIA Reviewer (name, job title, base and contact details)** Vickie Shaw, H&S Advisor and Security Lead
3. **Is it a Policy, Strategy, Procedure, Process, Tender, Service or Other?** Policy

Main Aims of the Document, Process or Service • Prevention and Detection of crime • Public safety • Maintenance of the public perception of the Trust
Please indicate in the table that follows whether the document or process has the potential to impact adversely, intentionally or unwittingly on the equality target groups contained in the pro forma

Equality Target Group	Is the document or process likely to have a potential or actual differential impact with regards to the equality target groups listed?	How have you arrived at the equality impact score?
1. Age 2. Disability 3. Sex 4. Marriage/Civil Partnership 5. Pregnancy/Maternity 6. Race 7. Religion/Belief 8. Sexual Orientation 9. Gender re-assignment	Equality Impact Score Low = Little or No evidence or concern (Green) Medium = some evidence or concern(Amber) High = significant evidence or concern (Red)	a) who have you consulted with b) what have they said c) what information or data have you used d) where are the gaps in your analysis e) how will your document/process or service promote equality and diversity good practice

Equality Target Group	Definitions	Equality Impact Score	Evidence to support Equality Impact Score
Age	Including specific ages and age groups: Older people Young people Children Early years	Low	Actions to be taken in event on an incident and measures to be proactive in security awareness.
Disability	Where the impairment has a substantial and long term adverse effect on the ability of the person to carry out their day to day activities: Sensory Physical Learning Mental Health (and including cancer, HIV, multiple sclerosis)	Low	Policy covers all groups and is adaptable if required to accommodate people's specific needs.
Sex	Men/Male Women/Female	Low	Actions to be taken in event on an incident and measures to be proactive in security awareness, not gender specific.
Marriage/Civil Partnership		Low	Actions to be taken in event on an incident and measures to be proactive in security awareness.
Pregnancy/ Maternity		Low	Actions to be taken in event on an incident and measures to be proactive in security awareness.
Race	Colour Nationality Ethnic/national origins	Low	Actions to be taken in event on an incident and measures to be proactive in security awareness, covers all national and ethical.
Religion or Belief	All Religions Including lack of religion or belief and where belief includes any religious or philosophical belief	Low	Actions to be taken in event on an incident and measures to be proactive in security awareness is not religion based.

Sexual Orientation	Lesbian Gay Men Bisexual	Low	Covers all groups.
Gender re-assignment	Where people are proposing to undergo, or have undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attribute of sex	Low	Not applicable.

Summary

Please describe the main points/actions arising from your assessment that supports your decision above A search has been conducted to view other Trusts and other NHS Organisations EIAs for this policy and all completed an initial screening assessment only with only one reference for the policy to be made available in other formats upon request.	
EIA Reviewer: V SHAW - H&S ADVISOR AND SECURITY LEAD	
Date completed: January 2023	Signature: V SHAW