Policy:

Closed Circuit Television (CCTV)/Surveillance Cameras (Inpatient and bed-based services) Policy

Executive Director Lead	Executive Director of Nursing and Professions.
Policy Owner	Head of Mental Health Legislation.
Policy Author	Human Rights Officer.

Document Type	Policy
Document Version Number	1.4
Date of Approval By PGG	29 January 2024
Date of Ratification	February 2024
Ratified By	QAC
Date of Issue	12/2023
Date for Review	05/2026

Summary of policy

To provide an unambiguous statement of the Closed-Circuit Television Policy applicable Sheffield Health and Social Care NHS Foundation Trust (SHSC) only as it is related to inpatient areas and bed-based services.

Target audience	SHSC staff

Keywords	Security, Access, Data & Information, CCTV, Privacy and dignity, Surveillance Camera, Recording

Storage & Version Control

Version 1 of this policy is stored and available through the SHSC intranet/internet.

Version Control and Amendment Log (Example)

Version No.	Type of Change	Date	Description of change(s)
1.0	New draft policy created	20/09/2022	New policy commissioned on 08/09/22 by Least Restrictive Practice Group following patient facing CCTV Audit. Much of guiding principles the draft emerged from the result of the audit data.
1.1	Draft for consultation with stakeholders	12/2022	Policy was presented to stakeholders with no changes requested from service users. Underlying human rights principles remained the same but the draft incorporated more on Data Protection obligations.
1.2	Policy for presentation at Policy Governance Group (PGG)	April 2023	Following PGG meeting several amendments/actions were mandated. •Highlighted sections need to be completed •Appropriate dates to be added •Ensure that those listed as 'responsible' are aware of their responsibilities. •List the Head of Mental Health Legislation as someone who has been consulted • More information to be added on how to support people who will now need to look at CCTV. • Look at the equality and diversity checklist with the EDI team •Fire and Security Officer and Health and Safety committee need to be consulted •Flow chart required expansion
1.3	Policy amended in line with the PGG requirements in April	07/2023	•Highlighted sections completed 07/23 •Dates added 25/07/23 •. Email was sent on 28/06/23 making

			those listed in the policy aware of their responsibilities. •The Head of Mental Health Legislation was consulted on 27/04/23 and had no further comments. •The HRO consulted with the DPO via email (15/06/23) to clarify training on how to support people who will now need to operate CCTV changes made to sections 6.7,10 and 12. •EDI elements were reviewed by Head of the EDI team and their feedback incorporated on19/05/23 •The Fire and Security Officer was consulted, and input incorporated on the introduction and clarification of the policy goals and function on 18/05/23. •The Health and Safety Committee approved the policy on 25/07/23.
1.4	Amendment to policy to reflect and clarify the practicalities of its operation	19/12/2023	•Definition of 'Intermittently observed CCTV' inserted into section 4 of the policy. •Seclusion rooms added to definition of non-communal areas •Changes to section 7.2 to provide practical framework for using Intermittently observed CCTV grounded in human rights principles. •Clarification of 'nominated staff' added to section 7.13 •Implementation plan brought up to date
2.0	Review on expiry of policy	05/2026	

Contents

Is there a plan to install or is there a currently an operating CCTV system in an inpatient or bed-based service area?

YES

Is this CCTV needed for one of the following reasons listed in Section 3 (a-e) of the policy?

YES

•CCTV cameras on inpatient wards or bed-based services, need to be lawful, justified and proportionate in terms of the Human Rights Act 1998.
•Each CCTV system will need to have a specific Standard Operating Procedure (see section 7.21(VI) of this policy).
•The camera must be situated in a place that is clearly visible and positioned in such a way that does not monitor areas not intended to be monitored.
•Move to next section…

Is the /will the proposed CCTV system situated in a non-communal area? A non-communal area is where a service users would have a reasonable expectation of personal privacy.

YES

• Executive level authorisation will be required to proceed with using a CCTV system in a non-communal area and justified again in terms of the Human Rights Act
• Monitoring stations to view live feeds of non-communal areas should (where possible) be situated separately from the areas where communal area CCTV monitoring stations are observed, and only limited numbers of staff should be assigned to observe these live feeds.
• Move to next section.

Is the CCTV footage to be recorded? (Note: As a matter of default footage should not be recorded).

YES

•If recording is deemed necessary, a separate additional assessment must be conducted to determine: that recording CCTV footage is lawful, justified, and proportionate in context of Article 8 of the Human Rights Act 1998 Trust's Recording Policy must be consulted to maintain human rights and data governance

•DPA guidance needs to be consisted 7.8-7.22 of the policy.

All CCTV cameras must be entered on to the CCTV register. Contact the Human Rights Officer to do this.
Move to next section…

Suitable warning signs must be displayed so that persons are aware that they are entering an area which is covered by surveillance equipment. Staff should discuss the presence of CCTV with patients/ residents their family/ carers and the impact it may have, at the time of admission if possible, or as soon as possible afterwards.

End.

NO

There is no need to consult this policy.

NO

A CCTV system on an inpatient ward or bed-based service setting is unlikely to be justifiably needed.

NO

•Move to next section…

NO

•Cameras should be monitored live and sited and operated as per section 7 -7.7

•Move to next section…

1 Introduction

This policy has been devised to help staff identify if there is a need for CCTV use in in-patient facing areas and bed-based services operated by the Trust and how that can be operated in accordance with legal requirements and national guidance.

Where there is a need for CCTV staff must ensure:

- Any one subject to being monitored and/or recorded by CCTV is told in a way they can understand, usually by displaying signs, which must be clearly visible and readable and the supply of information to service users via leaflets etc. Adaptation to individuals' communication needs will need to be considered.
- There is appropriate and legally compliant control of who can see monitoring stations (monitors broadcasting images) and who can access any recordings.
- The system is only used for the purpose it was intended for - for example, for clinically justified purposes or detection of crime.
- That all staff identified as operators of systems must be suitably trained and competent.

CCTV can be used as a measure to prevent criminal activity and minimise the likelihood of injury or harm occurring to patients, staff, visitors, and other to relevant persons for which a duty of care is held.

Where CCTV systems are installed and used, full consideration must be given and documented in regards to the privacy, dignity and human rights implications that the presence of CCTV might generate in the context of a clinical environments.

This policy outlines provides instruction for staff when they are considering a need for CCTV in inpatient setting and bed-based services (such as care homes).

The policy also recognises that this is an area where human rights in inpatient and bed based settings overlaps with the statutory requirements around data protection and governance and thus connects both data governance and human rights in a single policy.

This policy is written with reference to and to be in line with the legislative frameworks that govern the use of CCTV, national guidance, the Information Commissioner's Office guidance and published material from third sector bodies that have a particular expertise in considering the impact of CCTV upon service users in mental health and social care facilities, (for example the Restraint Reduction Network.)The policy is also requires that CCTV use is subject to Data Protection Impact Assessment to ensure compliance to nationally required information governance standards.

2 Scope

2.1 This policy applies to CCTV inside inpatient wards and bed-based services settings only (including outside garden spaces) where SHSC owes a duty of care.

2.2 This policy is not applicable to external areas outside inpatient settings/bed-based settings (i.e., carparks, public walkways, entrance/exit doors and gates etc).

2.3 This policy is applicable to any inpatient ward/bed-based service CCTV system that is owned, under the control of, or operated by SHSC.

3 Purpose

This policy identifies the purpose of observed CCTV as to enhance safety from identified risks. Where areas are actively monitored via CCTV, this will enable service users, staff and visitors to be supported by ensuring that the monitoring staff member can alert appropriate staff to the need for rapid response to incidents considered likely to cause injury or harm and therefore minimise the impact of such occurrences on life, safety, the delivery of patient care, the environment and property. Recorded CCTV footage may be used in the investigation of criminal incidents.

Specifically, the use of CCTV is limited to monitoring areas where:

a) Patients may encounter a risk of injury or harm as a result of their own actions and/or behaviours (intended or unintended).

b) Patients may exhibit behaviours that challenge, which may result in violence, criminality, injury, and intimidation of other service users, staff and visitors.

c) It assists in the prevention, detection and investigation of crime and assists law enforcement agencies in the apprehension of offenders and minimise the occurrence of unlawful activities.

d) CCTV can also be used where it is deemed a less intrusive option than in-person monitoring. If a patient is under observation, an observer watching on camera in an exterior room may be less intrusive. For example, if someone needs to be monitored whilst trying to sleep, a camera may be better in such a situation than a staff member sat in the room of the person trying to rest. Thus, CCTV here would assist in providing better nursing care subject to discussion and agreement with the service user.

e) Deterrence in some circumstances. CCTV may have the effect of preventing and minimising conflict, crime, and risky behaviours where there is good reason to believe that these may occur. However, if the key aim of siting CCTV in a location is deterrence, it will need to be demonstrated that there is a tangible risk that could be deterred by the presence of a monitored/recorded CCTV camera.

4 Definitions

Active CCTV observation: Where CCTV footage is being observed directly by someone assigned to watch the live feed on the monitor on which the CCTV images are being broadcast. The live images being observed may also be recorded.

CCTV: Closed-Circuit Television: CCTV is an electronic surveillance system comprising cameras, monitors and, in some cases, image recording devices functioning within a closed-circuit where the signal is not openly transmitted as it is with broadcast television. The video cameras transmit the surveillance information to a set number of monitors and, in some cases, recorders.

Body-worn cameras are a variant of surveillance cameras which are worn by selected members of staff. Body-worn Cameras are not currently used at SHSC. If the Trust decided to use this technology in future this policy will need updating appropriately.

Communal areas: These are the areas of a ward/residential unit that are shared, used routinely by staff, service users, and visitors. For example, corridors, gardens, TV lounges, dining rooms, activity rooms etc. In general, communal areas are quasi-public spaces, in that they are areas where there cannot be a reasonable expectation of total privacy. In such a space it is accepted that the use and function of that space is open to others to move about in freely, without restriction. Or in the case of visiting rooms, there would be limited access for the general ward population, but other members of the public (visitors) could be reasonably expected to be in the space at the same time as patients using the facility.

Data Protection Impact Assessment (DPIA): An assessment made before any significant new processing of person-identifiable information or change to existing processing to ensure it complies with data protection regulations and to identify any risks the processing presents. A template for DPIAs is available from the Data Protection Officer. CCTV/surveillance camera installations will use the DPIA template provided by the Biometrics and Surveillance Camera Commissioner.

Data Subjects: A Data Subject is a person who can be directly or indirectly identified through personal data, such as name, location, ID number, or other specific factors. In relation to this policy, Data Subjects are the people whose images are being captured on CCTV cameras.

Intermittently observed CCTV: Live feed CCTV is part of an overall system of observation and safety on each ward. It is present (where approved) in the context of other safety systems such as engagement and observations levels, staff presence in main ward areas, alarm systems and as such are in addition to these measures. Some cameras can be intermittently observed. This means that there is not an assigned member of staff required to be keeping constant watch on the live feed. Intermittently observed live feeds should be checked-on throughout the day by authorised staff, as the justification for CCTV use at all is that there is an identified risk that the camera is used for in the first place. However, it is

recognised that the risk factors for which the use of CCTV is sometimes designed to address are fluid and that there may be times when the need for constant observation is less necessary than at other times. Intermittently observed cameras can only be used in communal areas where there is not a reasonable expectation of total privacy (for example, corridors, gardens, visiting areas etc). They might be recorded or non-recording cameras. Intermittently observed cameras cannot be used where there is a need for constant monitoring of the live feed (such as seclusion rooms- these will have to be actively observed). It should be noted that from a service users perspective that any camera on the ward may be assumed to be under constant active observation and the operational distinction between intermittently observed and actively observed CCTV is not one that will be made by service users. This should be factored into the use of intermittently observed CCTV as the perception of being actively observed can be detrimental to some service users sense of privacy and dignity.

Non-communal areas: These are areas where there would be a reasonable expectation of personal privacy for the person occupying that space. For example, a person's bedroom, the lavatory, the shower/bathroom etc. In context of a mental health ward such private spaces might also include areas where staff have an individual under some form of observation; but that observation would be limited only to the staff assigned to attend to the patient - for example, de-escalation suites, seclusion rooms, or the observation windows in bedrooms.

Non-communal areas are thus defined here as private, in so much as the person in that space can expect not to be observed by anyone other than the limited number of staff specifically assigned to care for them whilst in that setting.

Non-recording CCTV: CCTV that provides video feeds only in real time to monitoring stations but does not record the footage captured by the camera.

Recorded CCTV: CCTV footage, which is stored on a recording device, which can then be viewed at a later date.

5 Detail of the policy

CCTV in inpatient units and bed-based services is a tool to help manage the identified risks that service users, staff and visitors to our units may encounter listed in section 3 (a-e) CCTV inside inpatient units and bed-based units can have important benefits including the ability to enhance the safety and security of patients, visitors and staff. It can sometimes be a less invasive means of monitoring and protecting against harm than in-person monitoring. However, it can also pose risks to privacy and dignity.

Balancing patients' human rights to autonomy, dignity and privacy with patient and staff security and safety is a key priority. CCTV in inpatient units and bed-based settings is a restrictive practice, and as such should only be used for specific purposes where the benefits of its use demonstrably outweigh potential harms.

CCTV is an alternative option to in-person monitoring but not a substitute for it. When it is used, CCTV must be a demonstrably preferable option to in-person monitoring in the specific circumstances in which it is applied. It needs to be shown to be less restrictive and/or safer and be a more effective alternative to in-person monitoring.

This policy sets out principles for the use of CCTV in inpatient units and bed-based settings to ensure that they meet national guidance and legal requirements.

6 Duties

6.1 The Chief Executive Officer (CEO)

The CEO is accountable for the manner in which the Trust implements the CCTV policy and adheres to agreed Data Protection requirements.

6.2 The Caldicott Guardian

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 information and ensure that service users' rights to confidentiality are respected.

6.3 The Senior Information Risk Owner (SIRO)

A SIRO is an Executive Director or member of the Senior Management Board of an organisation with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO is responsible for the overall management of the Trust's CCTV systems, the information risk aspects and compliance around using CCTV systems

6.4 The Data Protection Officer (DPO)

The DPO is responsible for advising on the application of the Data Protection Act 2018 and the UK General Data Protection Regulation. The DPO supports Trust wide Data & Information governance in accordance with UK GDPR, NHS Digital & England guidance, and the Data Security & Protection Toolkit in conjunction with the Information Governance Manager.

6.5 The Director of Nursing in consultation with the Clinical Director or the Head of Nursing

The DON and CD/ HON are responsible for approving and monitoring patient facing CCTV for use in specific service areas. The Clinical Director and the Head of Nursing are responsible for ensuring that all managers in their areas are aware of the policy and support its implementation.

6.6 The Information Asset Owner (IAO)

Each CCTV/surveillance camera system constitutes an Information Asset, and each system will have a nominated Information Asset Owner. The IAO will usually be a Ward/Team/Department Manager. They will be responsible for ensuring that this policy is fully implemented within the environment/the team/the department that they manage. They must ensure that the policy is readily available to all staff at all times. Managers must ensure that the documentation and auditing is completed in line with this policy. Managers must respond appropriately to any concerns regarding the implementation of this policy within their service area. Ward/Team/Department Managers must ensure regular review of the operation and functioning of the system.

The IAO is responsible for ensuring that:

a. Only authorised persons have access to data (physical security of the system under their control).
b. The CCTV/surveillance camera system has a specific Standard Operating Procedure (SOP) to cover use of the system.
c. An appropriate CCTV Maintenance Log is completed whenever any maintenance work takes place, giving the date and time of work.

6.7 The Information Asset Manager (IAM)

The Information Asset Manager is the person(s) authorised by the IAO to be the member of staff responsible for day-to-day operation of the CCTV equipment and is appropriately trained in the operation of the system. Training is usually obtained initially from the supplier to IAO and IAM, who then pass on this training to colleagues as appropriate.

6.8 Staff and volunteers

Responsible for compliance with Trust policy and reporting of any incidents

7 Procedure

7.1 Justification of Need

When proposing to use CCTV cameras on inpatient wards or bed-based services, the following questions should be answered and documented:

a. What reason is there for this surveillance? This will need to be one of the purposes listed in Section 3 a-e of this document.
b. How long will this surveillance last?
c. When will it be reviewed?
d. What alternatives might there be that are less rights-restrictive?
   i. CCTV is a blanket restriction, unless there is a demonstrable case for the legality, justification, and proportionality of this for everyone on the ward's safety and care.

7.2 CCTV should generally not be used unless cameras are being actively observed or recorded. However, risk factors are fluid and can change quickly and unforeseeably

depending on the dynamics and population of the ward at any particular time. Where the risk element is deemed to be lower at some times than at others CCTV can be intermittently observed. This means that staff do not have to keep constant watch of CCTV live feeds from communal areas of the ward (such as gardens, TV lounges etc) but can check the live feed intermittently. However, if upon review staff find that the camera is not needing to be checked at all, then ward governance should review whether there is a need for a live feed camera in that location at all.

7.3 Siting of Cameras

I. Fixed CCTV cameras will be sited in prominent positions where they are clearly visible.

II. Where CCTV cameras are installed, they need to be positioned for a demonstrably specific purpose (the aforementioned safety, security, and investigative purposes listed in Section 3 a-e of this document).

III. CCTV Cameras will not be sited, in such a way as to monitor and/or record areas that are not intended to be subject to surveillance.

IV. An assessment as to suitability should include consideration of the Human Rights Act 1998, in particular Article 8 - the right for respect for private and family life, home and correspondence. Any proposed installation should take into account the following questions:

Is the positioning of a CCTV camera lawful, justified, and proportionate?

- Lawful means that there is Lawful means that there is a legal framework that permits a proposed restriction to be made. Examples may be the Mental Health Act or Mental Capacity Act, but each situation and circumstance will need to be considered on a case-by-case basis. Specialist advice should be sought where necessary.
- Justified means there is a specified, justifiable aim for its use (safety, security, and investigative functions)
- Proportionate means that there needs to be a reasonable link between the aim of the CCTV's proposed use and the use of CCTV as the method to secure that aim.

CCTV cameras will not usually be sited in non-communal areas where individuals have reasonable expectation of privacy. This is especially the case where someone's dignity may be at risk, such as bedrooms, bathrooms and lavatories or where a person is in a situation where they are likely to be undressed. Any proposal to install CCTV in non-communal areas will need specific approval from an appropriate executive director.

V. Where CCTV is used in Multifaith rooms, particular consideration should be given to Article nine of the Human Rights Act (Freedom of thought, belief, and religion). Use of CCTV in Multifaith rooms will need to be justified and as lawful, justified,

and proportionate and justified in terms of one of the purposes listed in Section 3 a-e of this document.

7.4 Siting of Monitors

Monitors that relay footage from cameras from communal areas should be positioned in areas where they cannot be viewed by unauthorised persons - for example, in a staff office. They should not be visible to unauthorised persons - for example visitors to the ward, other service users or through windows by passers-by, etc.

7.5 All inpatient /bed based service CCTV needs to be listed on the patient-facing CCTV register (template in Appendix B).

7.6 Information provided to those under CCTV surveillance

I. CCTV must be overt and transparent – people must be made aware that CCTV is in operation, and it may only be used for clearly defined and specified purposes.

II. Suitable warning signs must be displayed so that persons are aware that they are entering an area which is covered by surveillance equipment.

III. The notices must be clearly visible and legible and contain the following information:

- Identify SHSC as the organisation responsible for the CCTV.
- The purpose of the CCTV surveillance.
- If the footage is recorded or being monitored.
- Details of whom to contact regarding the CCTV usage.

7.7 Staff should discuss the presence of CCTV with patients, their family/ carers on the ward and the impact it may have, at the time of admission if possible, or as soon as possible afterwards. Reasonable adjustments need to be made to accommodate for communication needs – such as translation into appropriate languages and/or the use of easy read, Makaton, Sign Language etc.

7.8 Recording of CCTV Footage

As a matter of default, CCTV footage should not be recorded in inpatient settings. Recording CCTV footage is only justifiable in limited circumstances where it can be demonstrated that recording actively serves one or more of these purposes:

- actively enhances the safety of service users or staff
- minimises or mitigates identifiable risks or harms (including deterrence)
- has clear and demonstrable potential to assist in the prevention or detection of crime

If recording is deemed necessary, a separate additional assessment must be conducted to determine:

a. that recording CCTV footage is lawful, justified, and proportionate in context of Article 8 of the Human Rights Act 1998.
b. that the need to record is the most appropriate choice after all other alternatives have been fully considered.
c. that the Trust's Recording Policy has been consulted with regard to how this can be done in keeping with human rights and data governance standards.

Similarly, by default there should be no sound recorded by the CCTV system. In cases where sound recording is deemed necessary, this should be detailed and justified in the above assessment.

7.9 Recordings containing person-identifiable information will be subject to the same requirements as other person-identifiable records. They must be stored securely, and access restricted on a need-to-know basis.

7.10 Retention periods are set out in the NHS Records Management Code of Practice, although surveillance camera recordings do not form part of the care record - any information from the recording which is relevant to the care record of service users must be transcribed separately into the care record. See the section on access and disclosure to data subjects below.

7.11 Covert use of CCTV (recorded or unrecorded) is subject to a Trust-wide blanket prohibition. Any use of covert CCTV would only ever be considered in exceptional circumstances and requires executive-level authorisation. If such recordings were felt to be necessary for the investigation of suspected serious malpractice or a criminal offence, this would need to be approved by the Senior Information Risk Officer or Caldicott Guardian in conjunction with NHS Counter-Fraud and would be subject to the Regulation of Investigatory Powers Act 2000. Any such recording would be for a specific, documented purpose and for a limited timeframe.

7.12 Turning CCTV on and off

In some circumstances cameras can be deactivated/reactivated. This can be a useful tool for enhancing privacy. When it is activated /deactivated the person(s) on whom the camera is trained should be informed of this status.

7.13 Access to live feed video of communal areas

Access to each CCTV system will be controlled by the designated Information Asset Owner (IMO), usually the Ward Manager. On a day-to-day basis the CCTV system will be operated by a nominated individual (Information Asset Manager - IAM) or an assigned member of their team, as specified in the Standard Operating Procedure for the system. These staff will be appropriately trained in operation of the system.

The viewing of live CCTV images and recordings will be restricted to the nominated staff members(this will usually be the clinical staff on duty at that particular time). No other

individual will have the ability to view or access any CCTV images unless in accordance with the terms of this policy regarding disclosure of images. CCTV systems will be checked daily by the IAM to ensure the system is operating effectively. Both IAO and IMO should identified by name, to ensure that there is a record of those who have had access to cameras.

7.14 Monitoring live feed footage from non-communal areas

I. In non-communal areas, only limited staff must be able to monitor the footage from these areas.

II. Monitoring stations of non-communal areas should (where possible) be separate from the monitoring stations that observe communal areas. The ability to see the live feed must be protected from the sight of anyone not specifically authorised/assigned (by the IAO) to see the feed. For example, monitors showing footage from non-communal areas should be in a different room where only the IAO and the designated IAM(s) have access. No other individual will have the right to view or access any CCTV images, unless in accordance with the terms of this policy as to disclosure of images.

7.15 Access to Recorded footage

I. No one other than the Information Asset Owner or Manager for the system is authorised to access any recorded footage – this includes viewing or downloading recordings

II. Where other staff require access to recordings, they will be required to submit a request to the Information Asset Owner with a justification on the basis of clinical/ safety/ security grounds. In cases of doubt, the request will be referred to the DPO and the Human Rights Officer.

III. Where external agencies require access to or copies of recordings they must submit a written request detailing the purpose for which it is made.

IV. Where the images are required for evidential purposes in legal proceedings, the images will be copied by the Information Asset Manager and stored on an encrypted storage device placed in a sealed envelope signed and dated and held by the IAO on site, or by an authorised person as directed by the SIRO, until completion of the investigations or handed to the relevant investigator. When sharing any recording the person accepting the recorded material must sign a declaration to the effect that they will be responsible for the security and destruction of the data once it is no longer required.

a. Where external investigators are allowed to view recorded footage rather than being provided with their own copy, the access will be documented and the system will be operated by the IAO or IAM.

b. Data exported from recording devices must be strictly controlled and destroyed when no longer required. All media containing CCTV images must be treated as confidential waste if disposal is required.

V. Where staff or service users request access to or copies of recordings of themselves this will be dealt with through subject access procedures – (at this address: https://www.shsc.nhs.uk/accessinghealthrecords).

7.16 Storage and Retention of Images

I. Data images recorded by CCTV will be retained only as long as necessary for the purpose for which they were originally recorded.

II. Recorded images will be stored for a maximum of 30 days unless there is a specific purpose for which they are required to be retained for a longer period, for instance investigation of an incident.

III. If recordings are required to be retained for longer than 30 days, the Information Asset Owner/Manager will flag the recordings for retention or make a copy for retention as appropriate to the system before the 30 days expires and recordings are automatically deleted.

IV. Recordings which are retained for the investigation of incidents will be deleted once the investigation of the incident is confirmed to be complete and the findings are finalised.

V. A Register of access to CCTV system recordings will be maintained by the Information Asset Manager to include:
   a. Date and time of access.
   b. Purpose of access.
   c. Name and job role of the person accessing recorded images

VI. The Trust will ensure that security measures will be implemented to prevent the unlawful or inadvertent disclosure of any recorded images. The security measures will include:
   a. CCTV recording systems being located within restricted access areas.
   b. CCTV systems will be encrypted/password protected.
   c. Restriction of the ability to duplicate copies of recorded images to specified members of staff.

7.17 Disclosure of and Access to Images to Data Subjects

I. Images of identifiable living people recorded within any CCTV Systems are personal information for the purposes of the DPA, which allows individuals the right to request access to or a copy of those images.

II. Access to recordings containing person-identifiable information are covered by Subject Access rights provided by Data Protection legislation. Subject Access Requests (SAR) are processed and monitored by the Access to Records team. Forms are provided on the SHSC website, (at this address: https://www.shsc.nhs.uk/accessinghealthrecords) to expedite the processing of requests but data subjects can make verbal requests to the organisation if they prefer. There is no fee for requests, and they should be answered within one month of receipt unless the request is complex, so staff should notify the Access to Records team promptly if they receive a request.

III. Any individual who requests access to images of themselves will be considered to have made a subject request pursuant to the DPA.

IV. When a Subject Access Request is submitted to the Trust, this will notified to the Access to Records team, who will advise the IAO on processing the request.

V. Where recorded information involves only the individual making the SAR then the individual may be permitted to view the recorded data; information will be strictly limited to the images of the individual making the request. The Information Asset Owner or Manager accessing the images must take appropriate measures to ensure that images of individuals other than the person making the SAR are not disclosed.

VI. If the recorded information contains images of persons other than the individual making the SAR, consideration will be given to whether:

a. The images of other persons can be obscured so as not to identify them.
b. The other individuals in the images have consented to the disclosure of the images or their consent could be obtained or;
c. If not, whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the SAR.

VII. A record must be kept and held securely of all disclosures which sets out:

a. When the request was made.
b. The process followed by the individual with access to the CCTV recorded images in determining whether the image contained third parties.
c. The considerations as to whether to allow access to those images.
d. The individuals that were permitted to view the images, when and:
e. Whether a copy of the images was provided and if so to whom, when and in what format.

7.18 Disclosure of Images to Third Parties

I. The Trust will only disclose recorded CCTV data images to third parties where it is permitted to do so in accordance with the DPA.

II. CCTV images will only be disclosed to law enforcement agencies in accordance with the purposes for which the system was installed.

III. If a request is received from a law enforcement agency for the disclosure of CCTV images, then the agency will be required to specify what images they require and the purpose they are required for. All information must be recorded in relation to any disclosure.

IV. In the event that an order is granted by a Court for disclosure of CCTV images, this should be complied with, giving careful consideration as to the exact details that the Court Order requires. In the event that concerns are raised regarding disclosure, the DPO must be contacted in the first instance and appropriate legal advice may be required.

V. If access has been authorised, two copies of the images supplied must be made, one made available for the third party (including law enforcement agencies), and one to be retained securely on site.

7.19 Misuse of CCTV

If misuse of the CCTV system is identified or suspected, this will be reported via the Trust incident reporting procedure.

7.20 Complaints relating to the policy

Any complaints relating to this policy or to any CCTV system operated by the Trust should be made in accordance with the Trust's Complaints Policy. Complaints in relation to CCTV images will be handled by the Information Asset Manager with responsibility for the CCTV System, and Corporate Affairs if requiring formal investigation

7.21 Planning New CCTV Systems

I. CCTV systems are intrusive and can risk human rights breaches. The decision to install CCTV must be informed by a risk assessment of the problems the system is intended to address as identified in Section 3, a-e. Alternatives to CCTV usage shall be explored as well as supportive measures such as controlled access to buildings. It is essential that due consideration is given to the need to maintain privacy and dignity, and all schemes should be assessed on their impact on people's Article 8 right to privacy and Article 3 consideration of inhuman and degrading treatment.

II. The Trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

III. Any proposed installation of surveillance cameras must be subject to a Data Protection Impact Assessment and must be approved by the Digital Assurance Group before it may commence operations.

IV. The Management Team and key stakeholders in the proposed new CCTV System should liaise and consult with the DPO to ensure that the any CCTV System is procured and installed in accordance with the operational requirement.

V. Any new CCTV System installed must be added to the Trust's Information Asset Register and included as a system to be maintained to ensure that the system is fit for purpose.

VI. Each CCTV system will have a specific Standard Operating Procedure which will include:

- Details of the Information Asset Owner (IAO) who has overall responsibility for the system
- Details of the designated Information Asset Manager or Managers (IAM) who has responsibility for the day-to-day operation of the system
- The specific purposes of the installation
- Backup and maintenance arrangements for the system
- Retention periods for any recordings made by the system
- Processes for answering subject access requests and other requests for accessing recorded material where appropriate, including the anonymisation of people identified on recordings when necessary

VII. Prior to the installation or repositioning of any CCTV camera or system, a Data Protection Impact Assessment DPIA) must be conducted by the system's Information Asset Owner to ensure that the proposed installation is compliant with legislation and ICO guidance. On completion of collating relevant information, the IAO must submit the assessment to the DPO for approval.

CCTV systems will use the DPIA template provided by the Biometrics and Surveillance Camera Commissioner. The for this can be found on SHSCs intranet system at this link: https://jarvis.shsc.nhs.uk/documents/data-protection-impact-assessment-dpia

VIII. Any new patient-facing CCTV must be added to the patient-facing CCTV register. Filling out the template in Appendix A and sending this to the Human Rights Officer (contact details in section15).

7.22 Existing CCTV Systems

I. All patient-facing CCTV must be added to the patient facing CCTV register (Appendix B).

II. All existing CCTV Systems will be managed on a day-to-day basis by the IAO and IAM authorised for operating the CCTV System.

III. The IAO and IAM must ensure that regular checks are carried out to ensure that the system is functioning satisfactorily, that the time recording function is accurate, screen images are not distorted, and must record and report any defects identified. All systems must be serviceable and function correctly.

IV. Any CCTV System updates required will need to be undertaken by the System-authorised contract engineers. Records must be kept of any checks carried out, when and by whom, and any identified faults should be reported as soon as practically possible to the contract engineer via the Estates Department. Where recording devices have to be taken off SHSC premises for maintenance or repair, arrangements must be made to ensure the security of any recordings stored on them. When recording devices are disposed of, any recordings stored on them must be securely deleted before they are removed from SHSC premises.

V. Images produced by the equipment must be as clear as possible in order that they are effective for the purpose(s) for which they are intended.

8 Development, Consultation and Approval

The Data and Information Governance Group raised concerns about use of surveillance cameras and whether they constitute blanket restrictions.

An audit of CCTV use in the inpatient units was requested by the Least Restrictive Practice Group (LRPG) to address concerns on potential overuse of CCTV. The LRPG dispatched Jonathan Phiri, the Patient Safety Officer (PSO) and Tallyn Gray, the Human Rights Officer (HRO) to arrange a visit to each inpatient ward. The PSO and HRO were tasked to inspect current patient- facing CCTV and to establish why CCTV is where it is, its purpose, whether it is live feed or recorded (or both) what information is given to service users and visitors, as well as governance and any privacy or dignity concerns.

The information from this was used in the development of a CCTV policy to address the gaps identified in Trust governance regarding inpatient facing CCTV.

The HRO consulted relevant stake holders (see table).

The drafts of the policy were presented to the Least Restrictive Practice Group and Data & Information Governance Board and amendments made. Reviewed drafts of policy via email and met with HRO over skype to discuss. The HRO incorporated input from this meeting in to the policy. The policy was reviewed against the Restraint Reduction Network guidance.

Stakeholder consulted	Consultation method
Security and Fire Officer	Information was provided by the Security and Fire Officer in the development of this policy 11/10/2022. Comments received and feedback incorporated in to section 1, 2.1 and 2.2, 3 7.1(a) and 7.2.(ii) (18/05/23).
Data Protection Officer	Reviewed drafts of policy via email and met with HRO over skype to discuss. Further revision and input received on 14/02/23 and then on 16/06/23. The HRO incorporated input into the the policy
Local Site – Nurse Managers, Business & Performance Manager & Governance Officers	HRO and Clinical Incidents Investigations Facilaitoar spoke with staff on all inpatiant units to carry out CCTV in inpatiant settings audit between July 13th 2022 and August 4th 2022.
Service Users	Draft of policy presnted to the Sun:Rise group on 22nd December 2022.The HRO incorporated input from this meeting in to the policy.
Reducting Restrictive Practices Lead	Reviewed drafts of policy via email and met with HRO over skype to discuss on 08/11/22. The HRO incorporated input from this meeting in to the policy.
Least Restictive Practice Group	Policy sent out for final review on 21/02/23 with no further comments added nor objections raised.
Data Information and Governace Group	Reviewed policy and reterned no comments/ objections on 21/02/22
Health and Safty Committee	The Health and Safety Committee approved the policy on 25/07/23.
Head of Mental Health Legistion	Reviewed policy and reterned no comments/ objections on 27/04/23
Head of Equality & Inclusion	Reviewed policy and reterned the policy on 19/05/23 and comments were incorpated into Appendix A and sections 7.3 (V),7.7, and 7.13.

9 Audit, Monitoring and Review

Monitoring Compliance Template						
Minimum Requirement	Process for Monitoring	Responsible Individual/ group/committee	Frequency of Monitoring	Review of Results process (e.g. who does this?)	Responsible Individual/group/ committee for action plan development	Responsible Individual/group/ committee for action plan monitoring and implementation
Review the register and new CCTV cameras being placed on it.	Review and audit	Least Restrictive Practice Group/ Human Rights Officer /Data Protection Officer	Biannually	Least Restrictive Practice Group	Least Restrictive Practice Group	Least Restrictive Practice Group/ Human Rights Officer Data Protection Officer

Policy review date: March 2026

10 Implementation Plan

The Human Rights Officer will assist frontline staff in drawing up SOPs. Key to this will be to ensure that patient information is provided in a way that is adjusted to the communication needs of service users, thus a patient information leaflet will be produced with input from EBEs and then translated into community languages and accessible formats.

11 Dissemination, Storage and Archiving (Control)

The policy will be made available to all staff via the Intranet and Trust website. A communication will be issued to all staff via the Communication Digest immediately following publication.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.0				
2.0				
3.2				
4.0	January 2024	January 2024	January 2024	

12 Training and Other Resource Implications

Departmental managers are responsible for ensuring that their staff are aware of and comply with this policy and that they are appropriately trained to use the systems required. Further information on this should be sought from the Trusts Data Protection Officer.

13 References and Links to Other Policies, Standards (Associated Documents)

Legislation:

Data Protection Act 2018/ General Data Protection Regulation (GDPR) 2018
Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 (PoFA)
Freedom of Information Act 2000 (FOIA)
Regulation of Investigatory Powers Act 2000
Human Rights Act 1998

SHSC Internal Policy Documents

Data & Information Security Policy

Data & Information Acceptable Use Policy

Records Management Policy

Confidentiality Code of Conduct

NHS Records Management Code of Practice

Recording policy

External Sources:

British Institute of Human Rights, 'Human rights and the use of cameras and other recording equipment in health& social care: A short guide' British Institute of Human Rights, 2021, p3 https://www.bihr.org.uk/Handlers/Download.ashx?IDMF=b1bee456-4c9e-4440-841a-494bb15bfdc3

CQC, 'Using Cameras Or Other Recording Equipment To Check Somebody's Care' (CQC, 28 June 2019)< https://www.cqc.org.uk/contact-us/report-concern/using-cameras-or-other-recording-equipment-check-somebodys-care>

CQC, 'Using surveillance in your care service', (CQC, 28 June 2019)< https://www.cqc.org.uk/guidance-providers/all-services/using-surveillance-your-care-service>

CQC, 'Using surveillance in your care service', (CQC, 28 June 2019)

Gov.UK, ‘Data protection and your business’ <https://www.gov.uk/data-protection-your-business/using-cctv)

Home Office: Surveillance Camera Code of Practice (2013)

Restraint Reduction Network, Surveillance And The Elephant In The Room’,(RRN 2021)https://restraintreductionnetwork.org/uncategorized/surveillance-and-the-elephant-in-the-room/

Restraint Reduction Network , Surveillance: A Restrictive Practice And Human Rights Issue(RRN 2001) p6 https://restraintreductionnetwork.org/wp-content/uploads/2021/09/RRN-Surveillance-Explainer.pdf

14 Contact Details

Title	***Name***	***Phone***	***Email***
Human Rights Officer	Tallyn Gray	0114 2263666	tallyn.gray@shsc.nhs.uk
Data Protection Officer	John Wolstenholme		john.wolstenholme@shsc.nhs.uk

Title	***Name***	***Phone***	***Email***
Head of Mental health Legislation	Jamie Middleton	(0114) 27 18110	jamie.middleton@shsc.nhs.uk

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement.

I confirm that this policy does not impact on staff, patients or the public.

I confirm that this policy does not impact on staff, patients or the public.

Name/Date: :

YES, Go to **Stage 2**

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3 – **Policy Revision** - Make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section

SCREENING RECORD	**Does any aspect of this policy or potentially discriminate against this group?**	**Can equality of opportunity for this group be improved through this policy or changes to this policy?**	**Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?**
Age	This policy has been reviewed in detail and no potential discrimination has be identified for this group.	**No specific impact identified.**	**No further action identified.**
Disability	So long as information is provided for in communication styles that is properly adapted- no further potential	**Information must be provided to accommodate for the communication needs of some patients.**	**Policy has been amended in Section 7.7 to require appropriate communication adjustments are made.**

	discrimination has been identified for this group.		
Gender Reassignment	This policy has been reviewed in detail and no potential discrimination has be identified for this group.	**No specific impact identified.**	**No further action identified.**
Pregnancy and Maternity	This policy has been reviewed in detail and no potential discrimination has been identified for this group.	**No specific impact identified.**	**No further action identified.**
Race	The policy is cognisant that some racialized groups maybe more likely to have had negative experiences of surveillance. This is especially so amount those who have experience as refugees fleeing from societies in which surveillance is used as a tool of state oppression. Thus CCTV, needs to be considered in terms of the impact it may have amongst these groups. This CCTV Policy will not discriminate against this characteristic.	**Information must be provided to accommodate for the communication needs of some patients who may be weary of CCTV due to past negative experiences. It is particularly important to ensure that information about the CCTV is provide in accessible language formats.**	**No further action identified. Policy has been amended in Section 7.7 to require appropriate communication adjustments are made. Furthermore, the implementation plan now calls for translation of patient information into community languages.**
Religion or Belief	This CCTV Policy will not discriminate against this characteristic.	**CCTV in Multifaith rooms could raise issues around Article Nine of the Human Rights Act- (Freedom of thought, belief and**	**Section 7.3 (V) requires that Article Nine considerations are reasoned in terms of lawfulness, justification, and proportionality when CCTV is used in Multifaith rooms.**

		religion).	
Sex	This CCTV Policy will not discriminate against this characteristic.	**Women may be more vulnerable to misuse of CCTV than men**	**Section 7.13 requires an additional safeguard to ensuring that the IAO and IAM are named individuals and there is a direct record of who exactly has had access to footage.**
Sexual Orientation	This policy has been reviewed in detail and no potential discrimination has been identified for this group.	**No specific impact identified.**	**No further action identified.**
Marriage or Civil Partnership	This policy has been reviewed in detail and no potential discrimination has been identified for this group.	**No specific impact identified.**	**No further action identified.**

Please delete as appropriate: - Policy Amended (see Implementation Plan)

Impact Assessment Completed by: Tallyn Gray, Human Rights Officer, 19/05/2023.

Appendix B

Patient facing CCTV register template

Ward /Site complex	Cameras	Monitoring Station/who can see the monitor	Has information been provided to SUs/visitors	Recorded- yes/no (if yes please explain why)	Justification- what risk is this camera addressing?	Last inspection	Privacy and dignity risk (HRA) Yes/no/maybe	Update

The CCTV register will be held by the Human Rights Officer, who is overseen by the Lest Restrictive Practice Group.

Appendix C

Review/New Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	✓
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit or other relevant bodies been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓

17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to i. review ii. audit compliance with the document?	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓