THE STATE HOSPITAL BOARD FOR SCOTLAND

CLOSED CIRCUIT TELEVISION POLICY

Policy Reference Number	SP04	Issue: 2.1
Lead Author	Physical Security Manager	
Contributing Authors	Deputy Physical Security Manager	
Advisory Group	Security and Resilience Group	
Approval Group	Policy Approval Group (PAG)	
Implementation Date	31 March 2023	
Revised Date	24 September 2024	
Next Review Date	31 March 2026	
Accountable Executive Director	Director of Security, Estates & Resilience	

The date for review detailed on the front of all State Hospital policies/ procedures/ guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/ procedure/ guidance at any time due to organisational/legal changes.

Staff are advised to always check that they are using the correct version of any policy/ procedure/ guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies/procedures can be found on the intranet: http://intranet.tsh.scot.nhs.uk/Policies/Policy%20Docs/Forms/Category%20View.aspx

REVIEW SUMMARY SHEET

No changes required to policy (evidence base checked)	☐

Changes required to policy (evidence base checked) ☒

Summary of changes within policy:

2023 Policy Review

Reflecting changes from the business case for new cameras to actual operational use.

Including:

- Addition of Appendix 2: Live CCTV monitoring of Modified Safe Room (MSR) / Seclusion Room.
- Appearance search.
- Introduction of the Privacy Masking System.
- Silver Command approval for use of Closed Circuit Television Policy (CCTV).
- Removal of previous Appendix 3: Protocol for editing images.

September 2024 revision

Section 7 updated to describe the capturing, retaining and copying of footage onto GDPR compliant digital devices. These include the previously described option of a USB device/memory stick, now included is the option of an encrypted external USB storage device and the use of Recordable DVDs and CDs.

CONTENTS

1 FOREWORD 4
2 PURPOSE OF CLOSED CIRCUIT TELEVISION POLICY 4
3 USING CLOSED CIRCUIT TELEVISION POLICY 4
4 EFFECTIVE ADMINISTRATION 6
5 SELECTING AND SITING CAMERAS 7
6 USING THE EQUIPMENT 8
7 LOOKING AFTER RECORDED MATERIAL AND USING THE IMAGES 8
8 DISCLOSURE 9
9 RETENTION 11
10 RESPONSIBILITIES 11
11 STAYING IN CONTROL 12
12 EQUALITY AND DIVERSITY 13
13 COMMUNICATION, IMPLEMENTATION, MONITORING AND REVIEW OF POLICY 14
14 STAKEHOLDER ENGAGEMENT 14
15 GLOSSARY 14
APPENDIX 1: THE GENERAL DATA PROTECTION REGULATION: DATA PROTECTION PRINCIPLES 15
APPENDIX 2: LIVE CCTV MONITORING OF MODIFIED SAFE ROOM (MSR)/SECLUSION ROOM 16
APPENDIX 3: MONITORING STAFF 17

1 FOREWORD

The State Hospital (TSH) has provided this Closed Circuit Television Policy (CCTV) policy in a similar format to that of the Information Commissioner for ease of reference and reading.

TSH use of CCTV has general public and political support and necessarily involves intrusion into the lives of individuals in and around the Hospital. The Information Commissioner's Office (ICO) research has shown that the public expect CCTV to be used responsibly with effective safe guards in place. Maintaining public trust and confidence in its use is important for benefits to be realised and for its use not to be viewed with suspicion.

Following the provisions of this code will help TSH to work within the law, fostering confidence and demonstrating that we take our responsibilities seriously in this regard.

2 PURPOSE OF CLOSED CIRCUIT TELEVISION POLICY

This code covers the use of CCTV and other systems, which capture images of identifiable individuals or information relating to individuals for any of the following purposes:

- To deter patients from escaping or attempting to escape.
- To deter those having criminal intent and to help reduce the fear of crime.
- To assist law enforcement agencies in the detection of crime, help apprehension and prosecution of offenders.
- To provide information and aid any TSH investigation.
- To give confidence to TSH patients, staff, volunteers and visitors that they are in a safe and secure environment.
- To provide TSH with information relating to vehicle traffic management.
- To monitor the movement of people.
- To monitor premises.
- To recognise people for entry or exit through specific points.
- To improve and provide information relating to Health and Safety matters.
- To see what an individual is doing, for example monitoring patient ground access.
- To establish facts.
- Training.

Most CCTV is directed at viewing and/or recording the activities of individuals. This means that use of CCTV in TSH must be operated in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA), the provisions of this policy and the ICO Code (see Appendix 1).

Note: This code does not cover the use of dummy or non-operational cameras.

3 USING CLOSED CIRCUIT TELEVISION POLICY

Using CCTV can be privacy intrusive, as it is capable of putting many people under surveillance and recording their movements as they go about their day-to-day activities.

The use of all CCTV installations in TSH must have benefits, and consideration to alternative solutions needs to be balanced against the effect on individuals.

CCTV is considered the most cost effective, reliable and least intrusive in comparison to some other methods of surveillance, for example replacing CCTV with additional nursing to staff to view all areas of the ward, or security staff to patrol the fence 24/7.

Patient Accommodation
General use: Yes.
A human target of 1.6m shall be displayed as a minimum of 25% screen height anywhere in the coverage area when viewed in the Security Control room (SCR) and the image shall have a minimum of 300 pixels/m pixel density at maximum target range.

Patient Bedrooms & Patient Shower Areas
General use: No. CCTV is not deployed.
Absolute exclusion: Yes. CCTV is prohibited in these areas.

Modified Safe Room (MSR)/Seclusion Room
General use: No.
Absolute exclusion: No. CCTV will only be live viewed for specific purposes and tasks Such as monitoring the patient's behaviour or mental state, reducing the risk of harm to himself or others. Recorded images will only be viewed after an adverse event has been recorded.

A human target of 1.6m shall be displayed as a minimum of 25% screen height anywhere in the coverage area when viewed in the SCR and the image shall have a minimum of 300 pixels/m pixel density at maximum target range.

Please refer to Appendix 2 for use of CCTV

Skye Centre, Family Centre, Tribunal Centre
General use: Yes.
A human target of 1.6m shall be displayed as a minimum of 25% screen height anywhere in the coverage area when viewed in the SCR and the image shall have a minimum of 300 pixels/m pixel density at maximum target range.

Patient Movement Areas
General use: Yes
A human target of 1.6m height shall be displayed as a minimum of 10% screen height anywhere in the coverage area when viewed in the SCR and the image shall have a minimum of 200 pixels/m pixel density at maximum target range.

Perimeter
General use: Yes
A human target of 1.6m shall be displayed as a minimum of 10% screen height anywhere in the coverage area when viewed in the SCR and the image shall have a minimum of 250 pixels/m pixel density at maximum target range

Car Park
General Use: Yes
A human target of 1.6m shall be displayed as a minimum of 20% screen height anywhere in the coverage area when viewed in the SCR and the image shall have a minimum of 200 pixels/m pixel density at maximum target range

Automated Number Plate Recognition (ANPR)
General Use: Yes
The system utilises specialist cameras to capture the data to ensure that an accuracy of recognition for UK or EU vehicle number plates, front and rear, on minimum 95% is achieved, regardless of weather or of ambient light levels.

The system will also capture video of the driver of the vehicle on entry, tagging that imagery and information to the recorded number plate. This data will be stored for a maximum of 30 days.

Access/Egress
General use: Yes
CCTV may be used at Access and Egress points, in conjunction with intercom or other appropriate technology. Identification standards should be met.

Other Areas
CCTV may be employed in other areas after a completed Business Case with full justification has been submitted and approval sought through The State Hospital Board. The Trade Unions and Professional bodies will be consulted where the installation of CCTV results in staff being under routine surveillance (see Appendix 3).

Where future demands for the use of CCTV and images arise they will be specifically addressed and a justified case provided to TSH Corporate Management Team. Where perceived intrusion occurs this should be recorded.

The systems are operated by TSH with particular consideration of the implications of the European Convention on Human Rights, Article 8 (the right to respect for private and family life). This includes:

- Systems established on a proper legal basis and operated in accordance with the law.
- Necessity to address a pressing need, such as public safety, crime prevention or national security.
- Proportionality to the problem.

Appearance Search
The system will include the ability to carry out an “appearance search” on footage, to allow selection of a target and an automatic search of recorded data to build a timeline” of activity. The system will also be used to manually track patients being escorted between buildings or for general surveillance on site

For patient unaccounted for, the Duty Security Manager must give permission for the system to be used.

For staff, Volunteers Visitor and Contractors who are unaccounted, the Security Manager will consult with the Duty Director

Privacy Masking
Any cameras that view outside of the desired field of view shall be fitted with electronic privacy zones. Electronic privacy is a means of masking regions of the field of view on the displayed camera image. The masking system shall dynamically adjust the size and position of the zone in accordance with motion control unit and zoom functions.

The privacy masking system configuration shall be protected to prevent settings being altered, bypassed or overridden by unauthorised persons.

Internal Grounds PTZs will be fitted with Dynamic privacy.
Perimeter PTZs are not fitted with Dynamic privacy, but in the rest position will point in to the perimeter. Any use of these cameras out with viewing the perimeter is not permitted unless in emergencies.

4 EFFECTIVE ADMINISTRATION

TSH have clear procedures in the operations and use of all CCTV systems within the site, based on this policy.

Establishing a clear basis for the handling of any personal information is essential and the handling of images relating to individuals is no different. TSH Head of Security or Nominated Deputy has the

responsibility for the control of the images to ensure that images are used and disclosed in accordance with TSH Policy. This practice also dictates what has to be recorded and to whom the information may be disclosed (see Section 7).

The Head of Security will have appropriate contracts in place with contractors to ensure the Hospital and Contractors are GDPR compliant.

Where there is a need to edit images in any way a pre-written process will be agreed with the Head of Security or Nominated Deputy, and the original images must be kept and sealed. Any editing of images must be carried out on a separate copy. The original images and first download must not be edited under any circumstance.

All images leaving TSH premises:

- Must be kept secure with a complete record of their location.
- Must be sealed when not in use.
- Must have a complete record of who carries out the editing, what has been edited and how it was edited.
- Must have written instructions of what requires to be edited, and what is expected of the edited image.
- For processing on behalf of TSH, such as editing, will only be provided to the processor where the use is governed by a contract or other binding agreement.
- The editing company must confirm that the person carrying out editing is appropriately trained and qualified to do so. The individual must have at least basic disclosure (Disclosure Scotland) and must be made aware of the confidentiality of the images.

The Head of Security or Nominated Deputy will ensure, and be able to demonstrate that every member of Control room staff knows the defined purpose of CCTV systems, how they operate and for what images can be used. All staff will undergo a local induction to ensure they have knowledge of this policy.

Standard Operating Procedures related to CCTV will be clearly documented and available to all control room staff. This includes how images are handled, disclosure guidance and record keeping (see Section 7).

It is the responsibility of the Head of Security or Nominated Deputy to ensure that proper procedures are followed in accordance with the GDPR, DPA, this Policy and the ICO CCTV COP.

The Head of Security or Nominated Deputy will appoint a person(s) to audit all CCTV procedures on a six monthly basis. The auditor shall provide a report to the Director of Security or Nominated Deputy, indicating what is in order, where there are doubts and what, if anything requires attention.

5 SELECTING AND SITING CAMERAS

Any CCTV images must be adequate for the purpose for which they are collected. It is essential that camera equipment and locations achieve the objectives for which they are intended. Both permanent and movable cameras should be sited and image capture restricted to ensure that they do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property. Where necessary software will be used to obscure private residences (see section 3).

The cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

Example: Check that a fixed camera positioned in winter will not be obscured by the growth of spring and summer foliage, or check that, at night it is not affected by glare from lighting columns.

Recording times for CCTV systems are pre-determined (see section 7). Any deviation from the time must be justified and notified to the Head of Security or Nominated Deputy.

6 USING THE EQUIPMENT

It is important that a CCTV system produces images that are of a suitable quality for the purpose for which the system was installed.

The recorded images must be stored in such a way that they cannot be inadvertently deleted or corrupted. Access should be recorded separately and logged.

Time and date synchronisation in all new installations will be linked to the atomic clock. All other installations will be checked and synchronised on at least a weekly basis.

On a six monthly basis the Head of Security or Nominated Deputy will ensure that, a quality check of the equipment is carried out, ensuring all cameras are facing the correct direction, that Rotakin results are still the same and that all recording is working effectively.

TSH CCTV system does not have audio and is not capable of recording conversation between people.

All Operations staff must be adequately trained in the use of the equipment, and with this Code of Practice.

Access to CCTV equipment is restricted to only those who need access, and have the delegated authority from The Head of Security or Nominated Deputy.

Patients on Grounds Access will be monitored at least every ten minutes to ensure the security of the hospital as well as their health and safety

Visitors will only be surviellled with approval by the Head of Security if concerns that the visitor may impact the good order of the hospital, the head of Security should document this decision and report same to the Director of Security.

7 LOOKING AFTER RECORDED MATERIAL AND USING THE IMAGES

<u>Storing and viewing the images</u>
Recorded material must be stored in a way that maintains the integrity of the image. This is to ensure that the rights of individuals recorded by the CCTV system are protected and that the material can be used as evidence in court. To achieve this TSH systems will be recorded onto hard disk and downloaded to an encrypted USB external storage device, CD or DVD as required.
Copies of recorded information will be controlled and only made:

- In relation to incidents which are the subject of any legitimate investigation.
- In relation to a valid request.
- For training purposes.
- For maintenance purposes.

Copies will only be issued by The Head of Security or Nominated Deputy.

Original recordings from which copies have been made will be stored securely on a GDPR compliant, encrypted USB external storage device. Such recordings will be clearly labelled, will be held in a secure manner and will only be accessible to persons directly concerned with achieving the objectives of the Code of Practice

Duplicate copies will be magnetically erased or physically destroyed upon written confirmation of the closure of the relevant investigation unless there is a formal objection from any party. The original downloaded recording will be kept for a period of at least one year if there are Health and safety issues, after which the Head of Security or Nominated Deputy will make a judgement on the need for retention, and if further retention is required set a new review date no more than 1 year from the last date of review.

CCTV information held by The State Hospital will not be retained indefinitely.

When information requires to be downloaded, the video information on hard disk should be downloaded on to an encrypted USB external storage device for retention and for legitimate sharing purposes to CD's, DVD's or a USB external storage device and sealed in evidence bags. Third party face redaction software will be available to edit CCTV footage.

Third party face redaction software will be available to edit CCTV footage

Erasure
Where the recording medium is hard disk, it will generally be automatically overwritten by the equipment.

Viewing
Viewing of live images on monitors will be restricted to the operator in the Control Room and staff in the incident command room, reception desk and vehicle lock. Live images can be viewed for the MSR/Seclusion Room from the night station within the wards (see Appendix 2).

The display of CCTV images in any other areas must have the prior approval of the Head of Security /Nominated Deputy and/or TSH Corporate Management Team, with the requesting person having completed an Operational requirement and Risk Assessment.

During Level 3 incidents the Silver Commander approve viewing by others as necessary including law enforcement.

Recorded images may also be viewed in a restricted area, such as a designated secure office. Viewing of any images in TSH will be regarded as private and only viewed by authorised people.

The location of monitors will be such that they cannot be seen by third parties.

Notification will be given, when appropriate, to The Manager in the area that footage is being or has been reviewed.

8 DISCLOSURE

Disclosure of images from the CCTV system must also be controlled and consistent with the purpose for which the system was established.

Individuals whose images are captured by a CCTV system have the right to obtain a copy of the information held by the system promptly. This right does not include providing other peoples' information.

Release of any images to the media must have the authority of the Director of Security or Nominated Deputy.

Note: It is likely to be acceptable to disclose images to law enforcement agencies if failure to do so would be likely to prejudice the prevention and detection of crime.

Any other requests for images should be approached with care, as a wide disclosure of these may be unfair to the individuals concerned. In some limited circumstances it may be appropriate to release images to a third party, where it is lawful to do so.

Evidence handling

Use of Video Data:

- The recording medium will be USB external storage devices, which may be directly recorded or downloaded from a hard disc.
- All USB storage devices must have unique identification numbers.
- On removing the medium on which the images have been recorded for use in legal .proceedings the operator must ensure that the following is documented.
- The name of the person who inserts and removes the images.
- The date and time of the incident.
- The location of the incident.
- The date and time the images were removed from the general system.
- Who has seen the recording, where and when, names and employers.
- The reasons for viewing.
- The outcome, if any from viewing.
- The reason the images were removed from the general system.
- Any crime or incident reference numbers.
- The location of the general equipment.
- The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.
- The name and business location of any person who is in the images or copies of the images;
- A signature from the recipient, with date and time.
- The recording must be viewed as soon as possible to determine if the evidence is needed on USB storage device. Any medium must be kept in a secure place. Unauthorised access must not be permitted.
- Where recording is on hard disk two copies should be downloaded on to the desired medium, one kept by TSH in a secure location and one provided to the Police or Procurator Fiscal.
- If the USB storage device requires to be moved from store prior to its handling to the police, a detailed log of timings and witnesses should be kept as this is likely to be the subject of cross examination.

USB storage for evidence will be segregated from duplicate recordings, sealed in a tamper proof evidence bag together with the associated incident report and stored securely. Such media will be accessible only to persons directly concerned with achieving the objectives of this policy. No such original media will be passed to any third party without the appropriate authority. The original recording and all copies made of the recording will be erased or physically destroyed upon written confirmation of the closure of the relevant investigation unless they are Health and safety issues or there are formal objections to destruction.

All operators and employees with access to images should be aware of the procedure, which need to be followed when accessing the recorded images.

Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment.

Access to the recorded images will be restricted to the Head of Security /Nominated Deputy or designated members of staff who will decide whether to allow requests for access by third parties in accordance with The State Hospital's documented disclosure policies (Sixth Data Protection Principle). (It is recommended those USB storage device evidence are handed to the police as soon as possible. The police will then become responsible for its security).

Viewing of the recorded images should take place in a restricted area, for example, in a manager's or designated member of staff's office. Other staff should not be allowed to have access to that area when a viewing is taking place (Sixth Data Protection Principle).

All operators should be trained in their responsibilities under this Code of Practice i.e. they should be aware of:

- TSH security policy e.g. procedures to have access to recorded images.
- TSH disclosure policy.
- Rights of individuals in relation to their recorded images.

Privacy Notices

A detailed Data Protection Impact Assessment (DPIA) has been approved for this policy and the following privacy notices can be found on the hospital intranet:

- Privacy Notice – Visitors to The State Hospital (Owned by Security and Person Centred Improvement Team).
- Patient Privacy Notice (Owned by Medical Records).
- Staff Privacy Notice (Owned by Human Resources).
- The General Public Privacy Notice is located on The State Hospital Website.

Time and Date Stamping

All recordings will, in the process of recording, be overlaid with the correct time and date. A known accurate point of reference will be used to set the time and date parameters. The time and date setting procedure will routinely take account of BST to GMT changeovers. Where the CCTV system incorporates more than one recording machine there will be a routine procedure to ensure synchronisation of the time and date display.

TSH has the discretion to refuse any request for information unless there is an overriding legal obligation such as a court order or information access rights.

When TSH has disclosed any image to another body, such as the police, they become the Controller for their copy of these images. It is their responsibility to comply with the GDPR and Data Protection Act in relation to their use and any further disclosures.

9 RETENTION

Recordings will not be kept for a longer period than is necessary to achieve the objectives of the system. This will generally be 30 days but the period may be extended where the system manager considers that there is reasonable and justifiable cause to do so. Where the recording system is on to a computer hard disk it may continue to run until the data is overwritten. Images should not be retained for longer than is necessary (Fifth Data Protection Principle)

Once the retention period has expired the images will be erased or removed. Where hard disk systems are used this may be automatically achieved by overwriting.

Where there is a need to retain images for longer, they should be downloaded onto to a USB device and TSH will keep a master copy. This is particularly relevant for any investigation.

10 RESPONSIBILITIES

Letting people know

Notices will be placed at the entrance of TSH reception areas clearly advising that the Hospital is under CCTV surveillance. Signs will be located at the entrance and reception area, but may be in other locations. Privacy notices are provided to all staff and visitors confirming that CCTV is in operation within TSH.

Subject access requests
Subject Access request will be managed under IG10 Subject Access Procedures.

Freedom of information
Freedom of Information requests will be managed under IG1 Freedom of Information Policy.

11 STAYING IN CONTROL

Once the guidance in TSH code has been followed and the CCTV system set up, the Head of Security or Nominated Deputy needs to ensure that it continues to comply with the GDPR, the Data Protection Act and the code's requirements in practice.

If requested staff should:
- Tell people how they can make a subject access request and who it should be sent to.
- Advise individuals to contact The Data Protection Officer if they have any complaints about the operation of the system or any failure of compliance with the TSH Code or Data Protection obligations.
- Advise individuals to write to the head of Security or Nominated Deputy if they have any other concerns regarding CCTV.

The Head of Security or Nominated Deputy must ensure that staff using the CCTV system or images should be trained to ensure they comply with this code.

In particular, they will know:
- What the organisation's policies are for recording and retaining images?
- How to handle the images securely?
- What to do if they receive a request for images, for example, from the police?
- How to recognise a subject access request and what to do if they receive one?

All images must be protected by sufficient security to ensure they do not fall into the wrong hands. This includes technical, organisational and physical security.

For example:
- Wireless systems will not be used without the authority of the Head of Security or Nominated Deputy. Where such systems are authorised they will have appropriate encryption.
- Copying of images will be restricted only to those authorised by the Head of Security or Nominated Deputy.
- When copies of images are made they will be *indelibly* marked and sealed in an evidence bag and kept as a "master copy" by TSH. A further copy will be indelibly marked and sealed in another evidence bag and provided in person to the intended recipient.
- The Recipient must sign to confirm receipt and provide that receipt immediately to the person delivering the images.
- TSH Control Room and plant rooms where images are recorded are in secure areas with restricted access.
- The Head of Security or Nominated Deputy will ensure that staff are appropriately trained and aware of consequences of misuse of the system and that such misuse will constitute a disciplinary offence.
- The Head of Security or Nominated Deputy must ensure that staff are aware that misuse of CCTV Images would constitute a criminal offence, beyond any TSH Action.

The Head of Security or Nominated Deputy will annually review all procedures in TSH to ensure they are up to date with the TSH Code of Practice, and to ensure that systems are maintained to the appropriate standard.

The Head of Security or Nominated Deputy, with the assistance of the Head of Estates, will annually ensure that the CCTV systems are effective and still doing what they were intended to do. If it does not achieve its purpose, it should be stopped or modified. If for any reason the purpose has changed that change must be recorded.

This Code of Practice, with information access requests, will be available on TSH intranet.

Any concerns relating to this area can be communicated to the Information Commissioners through the web site https://ico.org.uk/

12 EQUALITY AND DIVERSITY

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and / or discrimination.

The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person-Centred Improvement Lead on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments are in place to enable staff to understand and comply with policies and procedures. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

Patient pre-admission assessment processes and ongoing review of individual care and treatment plans support a tailored approach to meeting the needs of patients who experience barriers to communication (e.g. Dementia, Autism, Intellectual Disability, sensory impairment). Rapid access to interpretation / translation services enables an inclusive approach to engage patients for whom English is not their first language. Admission processes include assessment of physical disability with access to local services to support implementation of reasonable adjustments. Patients are encouraged to disclose their faith / religion / beliefs, highlighting any adapted practice required to support individual need in this respect. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

Carers / Named Persons are encouraged to highlight any barriers to communication, physical disability or anything else which would prevent them from being meaningfully involved in the patient's care (where the patient has consented) and / or other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy".

The volunteer recruitment and induction process supports volunteers to highlight any barriers to communication, physical disability or anything else which would prevent them from contributing meaningfully to patient care and / or engage in other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

13 COMMUNICATION, IMPLEMENTATION, MONITORING AND REVIEW OF POLICY

This policy will be communicated to all stakeholders within The State Hospital via the intranet and through the staff bulletin. The Person Centred Improvement Service will facilitate communication with Patients, Carers and Volunteers.

The Security and Resilience Group will be responsible for the implementation and monitoring of this policy.

This policy will be reviewed every three years or earlier if required.

14 STAKEHOLDER ENGAGEMENT

Key Stakeholders	Consulted (Y/N)
Patients	Y
Staff	Y
TSH Board	Y
Carers	Y
Volunteers	Y

15 GLOSSARY

CCTV: Closed Circuit Television: A TV system for private use, not for public broadcasting
Frame rate**:** Frequency in which video frames are displayed on a monitor, typically described in frames-per-second (fps). Higher frame rates improve the appearance of video motion.

ICO: The Information Commissioners Office https://ico.org.uk/

PTZ: Pan Tilt and Zoom.

RESOLUTION: Picture definition. Cameras, monitors, and VCR's can all have resolution specified in lines. A measure of the TV system to produce detail.

ROTAKIN®: A device to measure system resolution. A 1.6m black and white figure with test cards.

VMD: Video Motion Detection: A method of detecting movement on a screen to energise an alarm or start recording.

APPENDIX 1: THE GENERAL DATA PROTECTION REGULATION: DATA PROTECTION PRINCIPLES

The General Data Protection Regulation: data protection principles

Article 5(1)

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

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

Article 5(2)

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

This is not a full explanation of the principles. For more general information, see the ICO Legal Guidance at https://ico.org.uk/

APPENDIX 2: LIVE CCTV MONITORING OF MODIFIED SAFE ROOM (MSR)/SECLUSION ROOM

Live CCTV monitoring of Modified Safe Room (MSR)/Seclusion Room

This protocol should be read in conjunction with the seclusion policy, it refers to patients who are secluded in the MSR only.

Only staff authorised are permitted to view images on the monitor can do so, no other staff should have access to the monitor, to operate or view.

When in operation (live images viewable on the monitor) a sign will be displayed on the locked corridor door and those not involved in observation are not permitted to enter the area.

Should anyone not involved in the observation need to enter the area, then a telephone call will be made to the nurse observing the patient in the MSR to alert them. Observation via the monitor will be suspended/stopped whilst unauthorised persons are present.

A sign will be displayed on the corridor door stating live monitoring of the CCTV is in progress. Staff entering the area should notify the supervising nurse by phone that they will be entering the area with patients or are entering but not authorised to see live images.

Operation of Monitor

The key to unlock the control switch will be held by the Nurse in Charge.

At commencement of seclusion, the nurse assigned to observe the patient will be given the key to open the switch box to operate the monitor. No recording can be made at ward level.

The monitor displaying live images will not be left unattended.

If the observing nurse is unable to view the monitor for any reason, then the observation hatch on the Seclusion Room door should be utilised.

On confirmation that Seclusion has ended, (even if the patient remains in the MSR) then live monitoring must stop and the key returned to the Nurse in Charge.

APPENDIX 3: MONITORING STAFF

Monitoring Staff

Closed Circuit Television (CCTV) in The State Hospital (TSH) will capture pictures of staff (including appearance searches) even if they are not the main subject of surveillance. The purpose of the CCTV is described in section 2 of this code. There are no parameters in this code to monitor the amount of work done by any member of staff.

Cameras are directed to achieve the purpose for which they are intended and they are not directed specifically to capture images of staff. Cameras are not used for routine monitoring of staff. Deliberate viewing of staff, volunteers or visitors through CCTV footage without good reason is not an acceptable practice. It is considered gross misconduct, and could lead to termination of employment.

Images of workers may be used only if something is seen that cannot be expected to be ignored, such as criminal activity, gross misconduct, or behaviour that puts others at risk. If these images are used in disciplinary proceedings, the footage will be retained so that the individual can see it and respond.

If there are any cases where it may be appropriate to install CCTV specifically for workforce monitoring a decisions making process in compliance with the ICO code would apply, and the National TUS would be consulted.

Example: Goods are going missing from a storeroom. It would be appropriate to install CCTV in this room, as it will not involve continuous or intrusive monitoring and is proportionate to the problem.

Example: It is suspected that staff are making mobile phone calls during working hours, against hospital policy, and it is considered installing CCTV cameras on their desks to monitor them throughout the day. This would be intrusive and disproportionate.

Continuous monitoring will only be used in exceptional circumstances, for example, where hazardous substances are used and failure to follow procedures would pose a serious risk to life.

The only areas of TSH that are considered private in terms of CCTV monitoring are toilet areas, staff offices and patients' rooms with the exception of the Modified Safe Room.

Subject Access requests from staff will be managed under the IG10 Subject Access Procedure, which is the same way as subject access requests from all individuals are managed.

Staff should normally be aware that they are being monitored, but in exceptional circumstances, covert monitoring may be used as part of a specific investigation. Covert monitoring is where video or audio recording equipment is used, and those being monitored are unaware that this is taking place. Such monitoring is not covered by this Code of Practice and is subject to the Regulation of Investigatory Powers (Scotland) Act.

More advice on monitoring workers can be found in the ICO Employment practices code. The Employment practices code and other related guidance can be found on the ICO website: https://ico.org.uk/