Doncaster and Bassetlaw Teaching Hospitals
NHS Foundation Trust

Closed Circuit Television Policy (CCTV)

This procedural document supersedes: CORP/HSFS 34 v.1 – Closed Circuit Television Policy (CCTV)

Did you print this document yourself?
The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Sam Wilde – Chief Finance Officer
Author/reviewer: (this version)	Kerry Williams - LSMS
Date written/revised:	November 2025
Approved by:	DBTH Health and Safety Committee
Date of approval:	19 December 2025
Date issued:	24 December 2025
Next review date:	June 2028 (Policy valid until December 2028)
Target audience:	All Colleagues

Amendment Form

Please record brief details of the changes made alongside the next version number. If the procedural document has been reviewed **without change**, this information will still need to be recorded although the version number will remain the same.

Version	Date Issued	Brief Summary of Changes	Author
Version 2	December 2025	• Change of Executive Sponsor. • Section 2 purpose updated to include supporting Fraud and internal HR investigations. • Security training requirements monitored through the monthly KPI contract meetings. • Appendix 1 updated to reflect cameras on site.	Kerry Williams
Version 1	June 2022	New Policy please read in full.	Kerry Williams

Contents

Page No.

1 INTRODUCTION

The purpose of this Policy is to regulate the management, operation, and use of the closed circuit television (CCTV) systems managed and monitored by the external security contract provision covering Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust (The Trust) premises. The Trust is the responsible owner of the CCTV and conforms to the CCTV Data Protection Codes of Practice.

There are CCTV systems at various locations that are managed and maintained by Saba Parks UK. The systems comprise of a variety of camera types. The majority of cameras are reactively monitored within the Security Control Room and access to view images is limited to The Trust Local Security Management Specialist (LSMS) and Saba Multi Skilled Officers (MSO), (see Appendix 1 for guidance only).

This Policy adheres to the UK Data Protection Act 2018, and the UK General Data Protection Regulations 2021 (current data protection legislation) and will be reviewed on an on-going basis.

Ownership of the CCTV systems is listed separately (See Appendix 1 for guidance only).

2 PURPOSE

Within Trust premises, overt and covert CCTV can be used for the following purposes only:

- To protect Trust premises and Trust assets.
- To increase personal safety and reduce the fear of crime.
- To support the Police and other law enforcement agencies in reducing and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect staff, patients and visitors.
- To provide a deterrent effect and reduce criminal activity.
- To assist in the traffic management scheme (ANPR).
- To support internal HR investigations reviewed on a case-by-case basis.
- To assist internal fraud investigations

3 OWNERSHIP AND OPERATION OF CCTV

Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust is the 'data controller' for all CCTV systems operating within The Trust's sites.

The Trust is a 'joint data controller', as it shares its systems with Saba Parks UK, under an information sharing agreement. However the Trust determines the purpose for which and the manner in which any data are processed.

4 SCOPE

This policy applies to all persons employed by The Trust and any other groups, who access the Trust site, i.e. visitors, patients, contractors.

5 TRAINING/SUPPORT

All Security personnel must hold a valid Closed Circuit Television Licence and undertake renewal exam when required.

The training is contractual for the Car Parking, Security and Smoking Enforcement Contract with Saba Parks UK and training is monitored through the monthly KPI contract meeting.

Please note: The training requirements of staff will be identified through a learning needs analysis (LNA). Role specific education will be co-ordinated/ delivered by the topic lead. Alternatively, training may be accessed via an approved e-learning platform where available.

6 DUTIES AND REPSONSIBILITIES

6.1 Chief Executive

The Chief Executive has overall responsibility for ensuring that the Trust meets its statutory obligations that effective security management arrangements are in place and are periodically reviewed.

6.2 Director of Infrastructure

The Director of Infrastructure is the Trust Director who is the nominated Security Management Director (SMD), and they have overall responsibility for authorising the release of data when satisfactory documentary evidence is produced confirming legal proceedings, a subject access request, or in response to a Court Order.

6.3 Local Security Management Specialist

The Local Security Management Specialist (LSMS) has responsibility for security management and for the operational management of the Trust's security service.

6.4 Head of Information Governance/Data Protection Officer

Is responsible for advising the SMD & LSMS on systems and procedures that need to be in place to ensure compliance with this policy, the ICO's Code of Practice on CCTV, and on current data protection legislation.

The Head of Information Governance will ensure that the notification to the Information Commissioner relating to the use of CCTV equipment on Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust premises is maintained.

6.5 All Managers

All managers are responsible for:

- The development and adaptation of Trust Security procedures to ensure that they are relevant to specific Divisional, Directorate/Departmental needs.
- Overall supervision of the day-to-day security measures within their Division or Department.
- Ensuring that any incident of crime or suspected crime is reported without unreasonable delay via Datix and to the security team.
- Ensuring that appropriate education and training is provided for all staff.

6.6 All Colleagues

All Trust colleagues have a responsibility to ensure that they comply with relevant Security policies and procedures (see Trust extranet for policies).

All staff have a duty to protect NHS resources including our premises and equipment. If a crime or suspected crime is observed then the Security team must be alerted immediately by calling 2222.

It is also essential that all Security incidents involving or observed by staff are reported in accordance with the Trust's incident reporting procedure (Datix).

7 POLICY STATEMENT

In drawing up this policy, the following legislation has been taken into account:

- The Data Protection Act 2018.
- The UK General Data Protection Regulations 2021.
- The CCTV Code of Practice produced by the Information Commissioner.
- The Human Rights Act 1998.
- The Regulation of Investigatory Powers Act 2000.
- Caldicott Report 1997 & 2013.

All associated information, documents, and recordings obtained by CCTV are held and used in accordance with the current data protection legislation and the ICO's Code of Practice 2008.

The Criminal Procedure and Investigations Act 1996 places a statutory obligation on the police and other law enforcement agencies to record and retain material that may be relevant to an investigation. Relevant officers will err on the side of caution if they are unsure and seek to record and retain CCTV footage.

Images obtained from CCTV recordings will not be used for any commercial purpose.

Recordings will only be released to the media for use in investigation of a specific crime and with the written consent of the Police. Recordings will not be released to the media for purposes of entertainment.

Archived CCTV images will not be kept for longer than is necessary for the purpose of Police evidence. Once there is no longer a need to keep the CCTV images, they will be destroyed as confidential waste.

All associated information, documents, and recordings obtained and used by CCTV are protected by the current data protection legislation and are handled in accordance with the ICO's Code of Practice 2008.

Both Overt and Covert Cameras monitor activities on Trust premises, car parks and other public areas to protect Trust property and identify criminal activity whether occurring, anticipated, or perceived in order to enhance the safety and well-being of staff, patients, and visitors. All Security Officers are/have been made aware of this requirement.

When specifically authorised by the South Yorkshire Police (SYP), or Nottinghamshire Police (NNP), the Security Industry Authority (SIA) and prescribed officers stipulated by the NHS Counter Fraud Authority (see 8.10 of CORP/FIN 1 (D)), the Trust can engage in specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA).

Staff do not have any legal authority to direct CCTV cameras at an individual, their property, or a specific group of individuals.

The planning and design of CCTV systems has endeavoured to ensure maximum effectiveness and efficiency but cannot guarantee to cover or detect every incident occurring within the areas covered.

Warning signs, are displayed as required by the ICOs Code of Practice.

8 CONTROL ROOM

- The Security Supervisor/Control room operator will check and confirm the efficiency of the system daily and ensure that equipment is in full working order.
- Access to the CCTV Control Room will be restricted to authorised personnel only.
- Contractors and other visitors requesting entry to the Control Room will be subject to specific arrangements as outlined below.
- Control Room Operators must confirm the identity of any non-security personnel requesting entry to the Security Control Room and the reason for entry, if not clearly identified, access will be refused. To ensure that the operation of the Trusts CCTV systems is managed with the minimum of disruption, casual and non-essential visits by non-security personnel will not be permitted. All visitors must obtain permission to enter from the Security Supervisor and must be accompanied throughout the visit. Any visit may be immediately curtailed by the Security Supervisor if operational requirements deem this to be necessary (i.e. Incident occurring).
- In the event of an out of hour's equipment failure requiring access to the CCTV Control Room, the Control Room Operators must confirm the identity and purpose of contractors before allowing entry.
- A visitor's book will be maintained within the Control Room. Full details of visitors including time/date of entry and exit, and purpose of visit will be logged.
- At least one Security Officer must remain within the Control Room at all times if a visitor is present.

9 ARCHIVING PROCEDURES AND STILL IMAGES

In order to maintain and preserve the integrity of recordings for use in any future proceedings, the following procedures for use and retention must be strictly adhered to:

- CDs must be identified by a Name, Date, Time, Camera Location and Recording equipment used.
- The CD must be sealed, signed by the controller, dated, witnessed and stored in a designated secure unit.
- A log will be maintained in the Control Room detailing the release of CDs to the Police or other authorised applicants, and a register will be available for this purpose.
- Viewing of data images within the Control Room by the Police or other law enforcement agency must be recorded in writing and entered in the logbook. Requests by the Police to view images can only be actioned under current data protection legislation and the Police and Criminal Evidence Act (PACE 1984).
- If a CD is required as evidence, a copy may be released to the Police or other law enforcement agency.
- CD's will only be released to the Police or other law enforcement agency on the clear understanding that the CD remains the property of the Trust.
- The Police or other law enforcement agencies may require the Trust to retain stored CD's for possible future evidence. Such CD's will be indexed and securely stored until they are required to be produced as evidence.
- Applications received from external agencies (e.g. solicitors) to view archives/recordings must in the first instance be made to the Local Security Management Specialist. If appropriate and after liaison with the Director of Estates & Facilities CDs will only be released where satisfactory documentary evidence is produced confirming legal proceedings, a subject access request, or in response to a Court Order.

Still photographs of CCTV images should not be taken as a matter of routine. The taking of each photograph must be capable of justification (prevention of detection of crime).

All still photographs of CCTV images shall remain the property of The Trust and shall be indexed in sequence. A record is to be kept of the reason for production of the photograph, date, and time, the particulars of production of a live photograph, and information identifying the control room staff member responsible for producing the photograph.

Still photographs of CCTV images released to the Police or other law enforcement agency shall be dealt with as an exhibit and shall at no time be used for anything other than the purpose specified and identified when released to the them.

Still photographs of CCTV images shall not be kept for longer than is necessary for the purpose of evidence in criminal investigations. Once there is no need to keep the CCTV images, they must be destroyed as confidential waste.

10 BODY WORN VIDEO (BWV)

The Multi Skilled Officers based at Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust utilise Body Worn Video (BWV). Body Worn Video (BVW) equipment consists of a small camera

attached to the uniform of security officers which record visual and sound data by the officers during tours of duty.

Staff are not permitted to record with any other device other than those provided by Saba Parks UK.

The purpose of the recording is to safeguard staff, patients and the officers during violent and aggressive or anti-social behaviour incidents. The footage will be in an encrypted format, securely stored and only viewed by authorised persons.

The devices will only be activated during an incident in public or private areas (with due regard for patient and staff confidentiality as appropriate to the location and the event) and continuous recording is strictly not permitted. Data retention, review and disposal are in line with relevant legislation and current guidance.

Full Security Officer User instructions are included (see Appendix 2).

11 BREACHES OF POLICY

Any breach of the CCTV policy should be reported using the Trust's Incident reporting system Datix, which will alert the Trust Local Security Management Specialist.

The incident will then be investigated by the Saba Contract Security Manager in close association with The Trust's LSMS for further discussion and action as required.

Investigations following breach of the CCTV policy will result in recommendations to remedy the breach where appropriate.

12 COMPLAINTS

Any complaints concerning the Trust's CCTV system should be addressed to Local Security Management Specialist.

13 ACCESS BY THE DATA SUBJECT

Current data protection legislation provides Data Subjects (individuals to whom "personal data" relates) with a right to access data concerning them, including data obtained by CCTV.

Requests for Data Subject Access should be made on the appropriate application form available from the Saba Contract Manager.

Access to and disclosure of images is only permitted if it supports the purpose of the investigation. Under these circumstance, the request will be made to The Trust's LSMS where it will then be discussed with the Director of Estates and Facilities as to whether disclosure is appropriate, and whether or not there is a duty of care to protect the images of any third parties, taking advice from the Head of Information Governance/Data Protection Officer, or formal legal advice as necessary.

14 POLICY DEVELOPMENT AND CONSULTATION

This is a revised policy and ratified by the Trust Health & Safety Committee.

15 IMPLEMENTATION

This policy is implemented throughout the Trust and is available on the Trust website.

16 REVIEW

This policy will be formally reviewed in 3 years, or earlier depending on the results of monitoring, changes in legislation, recommendations from National bodies. There may also be an occasion as a result of a significant incident or accident, a complaint or a claim, data analysis or investigation.

17 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

The Trust's Security Management Specialist and the Saba Contract Manager will monitor the effectiveness of this policy.

All cameras will be maintained and serviced annually, and Saba will ensure that any operational software is security patched to date.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Working order and maintenance of equipment	Saba Contract Manager and LSMS	Equipment checks daily. Maintenance annually	Completed from CCTV control room. Repairs and maintenance will be reported immediately to Saba Parks UK
Requests to view footage	Saba Contract Manager	Quarterly	Reported to LSMS

18 DEFINITIONS

ANPR Automated Number Plate Recognition is the technology by which vehicles entering onto Trust premises are checked and identified against DVLA records IAW CCTV displayed notices.

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

19 EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27), the Equality Diversity and Inclusion Policy (CORP/EMP 59) and the Civility, Respect and Resolution Policy (CORP/EMP 58).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 3).

20 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

CORP/COMM 4 – Complaints Handling Policy (including Concerns)
CORP/FIN 1 (D) – Fraud, Bribery and Corruption Policy
CORP/HSFS 5 – Violence, Prevention and Reduction Policy
CORP/HSFS 15 – Security Policy – incorporating Bomb Threat / Suspect Packages
CORP/HSFS 22 – Electronic Door Access Control and System Policy
CORP/ICT 7 – Data Protection Policy
CORP/ICT 9 – Information Governance Policy
CORP/RISK 33 – Incident Management Policy
PAT/PS 1 – Missing Patient Policy
PAT/PS 19 – Abduction or Suspected Abduction of an Infant / Child Policy

21 DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

22 REFERENCES

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

APPENDIX 1 – TYPES AND OWNERSHIP OF CCTV SYSTEMS (FOR GUIDANCE ONLY NOT MANDATORY POLICY)

There are 377 CCTV cameras across the 3 Trust sites, reactively monitored from within the Security Control for the purpose of prevention and detection of crime and for staff, patient, and visitor safety.

In addition: -

Types of Cameras	**Numbers**
Static – internal & external	377

	General areas covered by CCTV	**Owned By**
1.	DBTH Grounds	Doncaster & Bassetlaw Teaching Hospitals NHS Foundation Trust
2.	Main Car Park	
3.	A&E	
4.	Main Entrance	
5.	Maternity	
6.	External Entrances & Exits	
7.	Under Croft	
8.	Mortuary	

APPENDIX 2 – EDESIX BODY WORN VIDEO

Booking out Equipment

All cameras will be stored in a secure area, in a suitable location along with any batteries and media cards. A supervisor will be responsible for maintaining the security of the cameras and the allocation to staff who have been instructed in its use. They should ensure that a suitable issue and returns log is available in order to show continuity if required, using the Daily Report book. When issued with the equipment the user should ensure that it is working correctly. This process should include the following basic checks:

- Unit is correctly assembled;
- Recording picture is the right way up;
- Sound recording level is appropriate to use;
- Date and time stamp is accurate.

Recording Events

Recordings should only be made in situations where the BWV wearer decides to take some form of action or make an intervention e.g. violence prevention. All recordings have the potential to be used in evidence even if it appears at the time that this is unlikely. It is important to record as much of an incident as possible. Recording should begin at the earliest opportunity at the start of an event.

It is crucial for the officer wearing the BWV camera informs the person(s), the surrounding staff / public that images and audio footage of the area is now being recorded. The officer must do this at the earliest, practical and safest opportunity using words similar to these or to the same effect:

'Sir / madam, your behaviour has now become unacceptable / threatening and you are now being recorded'

If the recording has started prior to arrival at the scene of an incident, the user should, as soon as possible announce to those present that recording is taking place and that actions and sounds are being recorded using words similar to these or to the same effect:

"Everything you say and do is being recorded on video".

Image Capture

At the start of any recording, the user should, where possible, make a verbal announcement to indicate why the recording has been activated. If possible, this should include: date, time, location, the nature of the incident, and the confirmation to those present that the incident is now being recorded using both video and audio recordings.

Unless circumstances dictate otherwise, recording must continue uninterrupted from the start of recording until the conclusion of the incident. It is advisable that the member of staff continues to record for a short period after any incident to clearly demonstrate to any subsequent viewer that the incident has concluded, and that the user has resumed other activities.

Prior to concluding recording, the user should make a verbal announcement to indicate the reason for ending the recording. This should state: the date, time and location; and the reason for concluding recording.

When an incident has been recorded, the officer must return to the control room to document and check video footage for quality. The BWV recording log must then be completed.

Selective Capture and Bookmarking

Selective capture is the user making a choice of when to record and when not to record. The nature of some incidents may make it necessary for the user to consider the justification for continuing to record throughout an entire incident. In cases where the user does interrupt or cease recording, they should record the decision including the grounds for making such a decision.

Transfer of images to BWV Evidence Management Software

Before completion of duty the BWV user will return the BWV camera to the shift Supervisor, who will transfer all data from the camera to the BWV Evidence Management software system for storage and retention. This will be managed by authorised personnel only.

Any recordings that require retention for evidence in court proceedings will be evidence and as such should be recorded as evidence through the BWV Evidence Management software. This footage will be retained in accordance with the organisation's requirements and in line with current legislation. Non-evidential footage should not be kept for longer than necessary to fulfil the purpose for which it was obtained in the first place. As best practice and to coincide with the main CCTV system, it shall be erased after 31 days.

Technical Standards

Release of Data

When a request for CCTV images has been requested this must be a written request within 28 days of the incident (due to non-evidential data being erased at 31 days) to the Trust and the person requesting the footage MUST bring relevant ID in relation to the request. At review/copy/seizure everything must be documented and witnessed, and only those who are lawfully entitled should be allowed to view it. Please ensure that no other person's confidentiality is broken. Contact must be made with the Trust for advice.

All Security staff must document on the BWV Review Log any recorded images that are to be reviewed by authorized persons, and on the CD/DVD Seizure log is to be used whenever the recorded images are burnt onto a disc to be taken away. The Logs are to be kept in the security office whenever CD/DVD footage is seized. A copy of these forms when a page is complete must be retained in the CCTV Evidence/Release cabinet.

All Security staff must be aware of their responsibilities under current data protection legislation.

Deletion of Images

There are no circumstances in which the unauthorised deletion by the user or other person of any images that have already been recorded can be justified, and any such action may result in legal or disciplinary proceedings.

All non-evidential data will be retained on BWV Evidence Management software (DEMS) for 31 days and then deleted automatically through the system.

Return of Equipment

When the BWV camera equipment is no longer required it will be returned to the appropriate storage facility, which is situated in the Security Control Room.

The user will ensure that all equipment is in working order and suitable for re issue. Any damage or malfunctions must be reported to the supervisor responsible for the equipment. Care should be taken to ensure that the device and any batteries are placed on charge for the next user.

Responsibilities: User

The User of the BWV will have received basic instruction in the use and legislation surrounding BWV prior to any use.

The Security staff member in charge of the BWV camera must sign a WORK INSTRUCTIONS form for the use of the body worn camera. This document will explain when to activate the Body worn camera unit and give guidance of when and how to provide credible evidence using the Body camera system. The document must be filed and kept within the Security control.

It is the responsibility of the BWV user to ensure that:

- Equipment is checked prior to deployment to ensure it is working correctly.
- That the batteries are charged prior to use (consider taking spare batteries) and immediately recharged on return.
- That the time and date settings are accurate.
- That camera lenses are clean, and the picture quality is suitable.
- The camera lens is aimed and focused appropriately to capture evidence.
- Compliance with legislation and guidance.
- View only footage they have a bona-fide reason for viewing.

Process Detail:

- All Security Officers must have undertaken the training required to operate the equipment/system.
- All Security officers on every working shift MUST when using a BWV camera complete the signing in/out sheet for continuity. This form must be kept in the security office.
- When an incident has been recorded the officer must return to the control room to document and check video footage for quality. The BWV camera recording log must then be completed.
- Release of footage must be in accordance to LOP.SEC004. CCTV & Data Protection.

RELEASE OF DATA/IMAGES MUST BE APPROVED AND PROCESSED BY: The Local Security Management Specialist

APPENDIX 3 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

Service/Function/Policy/Project/Strategy	Division	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Closed Circuit Television Policy (CCTV)	Estates & Facilities	Kerry Williams	Existing Policy	4 Nov 2025

1) Who is responsible for this policy? Name of Division/Directorate: Estates & Facilities

2) Describe the purpose of the service / function / policy / project/ strategy? Management of CCTV

3) Are there any associated objectives? Legislation, targets national expectation, standards: GDPR & DPA

4) What factors contribute or detract from achieving intended outcomes? – 24 hrs CCTV coverage

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] – N/A

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] –

6) Is there any scope for new measures which would promote equality? [any actions to be taken] N/A

7) Are any of the following groups adversely affected by the policy? No

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form – see CORP/EMP 27.

Date for next review: June 2028 (Policy valid until December 2028)

Checked by: Sean Tyler **Date:** 5 November 2025