Tameside and Glossop Integrated Care NHS Foundation Trust

Closed Circuit Television (CCTV) Policy

6.0

Management, operation, and use of closed circuit television

EQUALITY IMPACT

The Trust strives to ensure equality of opportunity for all both as a major employer and as a provider of health care. This policy has therefore been equality impact assessed by the Health and Safety Group to ensure fairness and consistency for all those covered by it regardless of their individual differences, and the results are shown in Appendix 3.

Version:	**6.0**
Authorised by:	**Secuirty Managment Group**
Date authorised:	**26th September 2018**
Next review date:	**September 2021**
Document author:	**Head of Facilities**

VERSION CONTROL SCHEDULE

management, operation, and use of the closed circuit television

Version : 6.0

Version Number	Issue Date	Revisions from previous issue
1.0 (final)	1st August 2006	Original issue. Approved by Trust Executive Group
2.0	5th March 2009	Amended to ensure compliance with NHSLA level 3. Changes include: More defined responsibilities i.e. who will monitor the policy and who they report to. Actions following an incident Monitoring Alerts Post Incident Review Ensuring compliance. Further amendments were made following review by TEG, they included formatting More definitions Changes to Trust Logo
3.0	7th April 2011	Amended details of Security Management Director, formerly this role was underatken by the Director of Planning and Performance. The role now falls under the remit of the Director of Human Resources. Removed the word Tape(s) from the policy, as these are no longer used.
4.0	5th Nov 2013	Information Commissioner CCTV Code of Practice, retrieved 12th June 2013 from: http://www.ico.org.uk/upload/documents/cctv_code_of_practice_html/1_foreword.html Deleted covert cameras from appendix 2 Added section regarding ownership and operation of CCTV. Included Information Governance Lead in list of Duties
5.0		Amended details of Security Management Director, formerly this role was underatken by the Director of Human Resources. The role now falls under the remit of the Director of Estate & Facilities.

		Replaced ‘Equality Impact Assessment Tool’, with ‘Analysis of Effects’
6.0		Incusion of Body Worn Cameras section Change Trust name This Policy adheres to the Data Protection Act 2018, previously 1998

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The purpose of this Policy is to regulate the management, operation, and use of the closed circuit television (CCTV) systems monitored by the Security Control covering Tameside and Glossop Integrated Care NHS Foundation Trust premises. Tameside and Glossop Integrated Care NHS Foundation Trust is the responsible owner of the CCTV Systems at the Tameside Hospital and conforms to the CCTV Data Protection Codes of Practice.

1.2 There are CCTV systems at various community locations that are managed by the landlord of the property, they include NHS Property Services, Community Health Partnerships (CHP) and LNM Healthcare.

1.3 The systems comprise of a variety of camera types. The majority of cameras are monitored within the Security Control Room and access to view images is limited to Security Staff (see appendix 1 for guidance only).

1.4 This Policy adheres to the Data Protection Act 2018, and the General Data Protection Regulation and will be reviewed on an on-going basis.

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

2. PURPOSE

2.1 Within Trust premises CCTV is 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 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

3. OWNERSHIP AND OPERATION OF CCTV

3.1 Tameside and Glossop Integrated Care NHS Foundation Trust is the ‘data controller’ for all CCTV systems operating on the Tameside Hospital site.

3.2 The Trust ‘data controller’ shares its systems with Engie, however the Trust determines the purpose for which and the manner in which any data is processed

3.3 The CCTV at community locations is owned by the landlords and include NHS Property Services and Community Health Partnerships (CHP) and LNM Healthcare.

4. SCOPE

4.1 This policy applies to all persons employed by Tameside and Glossop Integrated Care NHS Foundation Trust and any other groups, who access the Hospital site, ie: visitors, patients, contractors.

5. DEFINITIONS

4.1 Closed-circuit television (CCTV) 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.

6. DUTIES

6.1 Trust Board

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

6.2 Human Resources Director

The Director of Human Resources is the Trust Director with nominated 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 Head of Facilities

The Head of Facilities 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 Head of Facilities 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 the Data Protection Act 2018, and the General Data Protection Regulation. The Head of Information Governance & Policy Assurance will ensure that the notification to the Information Commissioner relating to the use of CCTV equipment on Tameside and Glossop Integrated Care NHS Foundation Trust premises is maintained

6.5 **All Managers**

are responsible for:

- The development and adaptation of Trust Security procedures to ensure that they are relevant to specific Directorate / Departmental needs.
- Overall supervision of the day to day security measures within their Directorate or Department.
- Ensuring that any incident of crime or suspected crime is reported to Security Department.
- Ensuring that appropriate education and training is provided for all staff.

6.6 **All Staff**

All members of staff have a responsibility to ensure that they comply with relevant Security policies and procedures (see Trust Intranet for policies). It is also essential that all Security incidents involving or observed by staff, are reported in accordance with the Trust's incident reporting procedure.

7. POLICY STATEMENT

7.1 In drawing up this policy, the following legislation has been taken in to account:

- The Data Protection Act 2018
- The General Data Protection Regulation
- 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

7.2 All associated information, documents, and recordings obtained by CCTV are held and used in accordance with the Data Protection Act and the ICO's Code of Practice 2008

7.3 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.

7.4 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.

7.5 All associated information, documents, and recordings obtained and used by CCTV are protected by the Data Protection Act and handled in accordance with the ICO's Code of Practice 2008.

7.6 Cameras monitor activities on Trust premises, car parks and other public areas to 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 of this requirement.

7.7 Except when specifically authorised by the NHS Protect, using specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA), staff must not direct cameras at an individual, their property, or a specific group of individuals.

7.8 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.

7.9 Warning signs, as required by the Code of Practice of the Information Commissioner are displayed at all access routes to areas covered by the Trust CCTV.

8. OPERATION OF THE SYSTEM

8.1 All CCTV Systems will be administered and managed by the Security Department, in accordance with the principles and objectives expressed in the Data Protection Act 2018, the General Data Protection Regulation, and the Commissioner's Code of Practice.

8.2 The day-to-day management of CCTV located at Tameside Hospital site will be the responsibility of the Security Department. All CCTV systems on sites other than Tameside Hospital are to be managed by the Clinic/Department in which the systems are located.

8.3 The Control Room will only be staffed by authorised Security Personnel.

8.4 The CCTV system will be operated 24 hours a day, 365/6 days a year.

9. CONTROL ROOM

9.1 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.

9.2 Access to the CCTV Control Room will be restricted to authorised personnel only.

9.3 Contractors and other visitors requesting entry to the Control Room will be subject to specific arrangements as outlined in 9.4 and 9.5 below.

9.4 Control Room Operators must confirm the identity of any non-security personnel requesting entry to the Security Control Room, and the reason for entry, and if not clearly identified, access will be refused.

9.5 To ensure that the operation of 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.

9.6 Any visit may be immediately curtailed by the Security Supervisor if operational requirements deem this to be necessary (i.e. Incident occurring).

9.7 In the event of an out of hours equipment failure requiring access to the CCTV Control Room, the Control Room Operators must confirm the identity and purpose of contractors before allowing entry.

9.8 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.

9.9 At least one Security Officer must remain within the Control Room at all times.

10. ARCHIVING PROCEDURES AND STILL IMAGES

10.1 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 must be recorded in writing and entered in the log book. Requests by the Police to view images can only be actioned under section 29 of the Data Protection Act 2018 and the Police and Criminal Evidence Act (PACE 1984)
- If a CD is required as evidence, a copy may be released to the Police. CD's will only be released to the Police on the clear understanding that the CD remains the property of the Trust.
- The Police 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 Head of Facilities. If appropriate and after liaison with the Director of Human Resources (or in the absence of the Director of Human Resources by the Director of Estates and 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.

10.2 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), and only done so with permission from the immediate person in charge i.e. line manager.

10.3 All still photographs of CCTV images shall remain the property of Tameside and Glossop Integrated Care NHS Foundation 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.

10.4 Still photographs of CCTV images released to the Police shall be dealt with by the Police as an exhibit and shall at no time be used for anything other than the purpose specified and identified when released to the police.

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

11. BODY WORN VIDEO (BWV)

11.1 The Security Officers based at the Tameside Hospital site 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.

11.2 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.

11.3 The devices will only be activated during an incident and continuous recording is strictly not permitted. The data will be processed and managed in line with Code of Practice and principles of the Data Protection Act 2018. Data retention, review and disposal is in line with relevant legislation and current guidance.

11.4 Full Security Officer user instructions are included in Appendix 2

12. BREACHES OF THE POLICY

12.1 Any breach of the CCTV policy should be reported using the Trust's Incident system. It will be initially investigated by the Assistant Security Manager for Engie, and then reported to the Head of Facilities for action.

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

13. COMPLAINTS

13.1 Any complaints concerning the Trust's CCTV system should be addressed to the Director of Human Resources.

14. ACCESS BY THE DATA SUBJECT

14.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relates) with a right to access data concerning them, including data obtained by CCTV.

14.2 Requests for Data Subject Access should be made on the appropriate application form available from the Head of Facilities

14.3 Access and disclosure to images is permitted only if it supports the purpose of the investigation. Under these circumstance the request will be made to the Head of Facilities and discussed with the Director of Human Resources (or in their absence of the Director of Estate and Facilities) as to whether disclosure is appropriate and whether 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

15. POLICY DEVELOPMENT & CONSULTATION

15.1 This policy was first authorised by the Trust Executive Group in August 2006.

15.2 The Policy has further development (see version control)

15. IMPLEMENTATION

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

16. MONITORING

16.1 The Security Management Group will monitor the effectiveness of this policy.

16.2 All cameras will be maintained and serviced annually ensuring that the software is up to date..

17. REFERENCES

17.1 http://www.ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.pdf

18. APPENDICES

18.1 The following appendices are attached to support the policy

Appendix 1 - Types and ownership of CCTV systems (for guidance only not mandatory policy)

Appendix 2 – Equality Impact Assessment Tool

19. REVIEW

19.1 This policy will be formally reviewed in 3 years, or earlier depending on the results of monitoring, changes in legislation, recommendations from National bodies, or as a result of incident or accident, complaints or claims data analysis or investigation.

Appendix 1

Types and Ownership of CCTV Systems (for guidance only not mandatory policy)

There are 143 CCTV cameras monitored from within the Security Control for the purpose of prevention and detection of crime and for staff, patient, and visitor safety. In addition, 17 cameras are monitored by individual Departments/Wards and are used in conjunction with Door Access Systems

Types of Cameras	**Numbers**
Dome (PTZ)	**30**
Static – internal & external	**113**

	General areas covered by CCTV	**Owned By**
1.	Tameside Hospital Grounds	Tameside Hospital NHS Foundation Trust and Cofely-gdfsuez
2.	Main Car Park	
3.	Multi Storey Car Park	
4.	Fountain Street	
5.	Automatic Barriers	
6.	Charlesworth Building	
7.	Ladysmith Building	
8.	Hartshead building (North and South)	
9.	Silver Springs	
10.	Renal Unit	
11.	Mortuary	
12.	Pathology	
13.	Door Access Controls	

Appendix 2

Engie 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: date, time, 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 organisations 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

The data captured via the Body Worn Cameras is secured by an encryption (AES256) coupled with password-controlled access levels and a full audit trail in the

DEMS software. The ENGIE Security Manager has overall responsibility and login details for the DEMS system. This ensures only the Security Manager has access to any data captured and the release of any data.

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 only those requesting the information 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 to document any recorded images that are to be reviewed by authorized persons and CD/DVD Seizure log to be used whenever the recorded images are recorded onto a disc to be taken away. Located in the security office when 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 the DATA PROTECTION ACT 2018 and ensure the data protection principles are adhered too.

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 back 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: Andy Wood to authorise after consultation and approval with the Trust.

Appendix 3
Analysis of Effects Assessment (AoE)

Title of Policy: Closed Circuit Television Policy (CCTV)

Short description of Policy The purpose of this policy is to regulate the management, operation and use of the CCTV systems monitored by Tameside and Glossop Integrated Care NHS Foundation Trust. The Trust is the responsible owner of the CCTV systems and conforms to the CCTV data protection codes of practice.

Date of assessment: 26th September 2018

Person responsible for assessment: **Steve Peet, Head of Security**
Is this a proposed new policy/proposal? **No** **Is this a review of an existing policy/proposal?** **Yes**

1. Who is responsible for the policy/proposal? *(Consider the following;* *i. Who is accountable?* *ii. Who implements it?* *iii. Who is responsible for policing/monitoring?* iv. *Who enforces the policy?)*	*Estates & Facilities*

2. Who are the main stakeholders in relation to the policy/proposal? *(Consider the following;* *i. Who needs to be consulted / informed about the policy/proposal?* *ii. Who is the policy/proposal intended to involve in the wider sense? For example; Staff/professionals, the public/community…*	This policy was approved by the *????*
3. What outcomes are expected / desired from this policy/proposal? *(Consider the following;* *i. Who will benefit from this policy/proposal and in what way will they benefit?* **ii.** *Does the policy/proposal explicitly involve the elimination of inequality, or the promotion of equality?)*	This policy has been developed by the Head of Security using advice issued by NHS Protect. This policy has been developed to support the provision of a safe and secure environment for patients, visitors and staff

4. The following section requires you to assess the likely negative impact and positive impact of your policy/proposal on the nine Protected Characteristics as defined by the Equality Act as follows. Please support any answers with evidence.		
Protected Characteristics	**Answers to:** **What likely adverse impact will this Policy / Service have on the public or staff, giving particular regard to potential impacts negative and positive in relation to:**	**Evidence:** ***(What is your evidence for this answer?*** ***Consider; both quantitative and qualitative existing data.)***
a. Race	Positive	The promotion of this policy will raise awareness to staff of their responsibilities. This policy applies to all those employed by and / or using the Tameside and Glossop Integrated Care NHS Foundation Trust site, including volunteers, students and contractors
b. Disability	Positive	As above
c. Sex	Positive	As above
d. Religion and belief	Positive	As above

e. Sexual orientation	Positive	As above
f. Age	Positive	As above
g. Carers	Positive	As above
h. Gender Reassignment	Positive	As above
i. Marriage & Civil Partnership	Positive	As above
j. Pregnancy & Maternity	Positive	As above
K. Human Rights	Positive	As above
5. Is there any further evidence / data that you would consider relevant or necessary in order to answer the above question? If so, please detail. *	Not applicable	
6. Are any of the above impacts (detailed in 4a – K) justifiable, valid or	None	

legal? **Please explain?**	
7. Is this policy/proposal missing a valid opportunity to promote equality of opportunity for one or more of the groups (see 4a) concerned? Please expand.	Not applicable
8. Based on the above, do you consider that this policy/proposal now requires a full impact assessment?	Yes – outlines employee/management responsibilities in the policy.

Signed (Responsible Manager for Policy/proposal)……
Date…….