Tees, Esk and Wear Valleys
NHS Foundation Trust

CCTV Policy

CORP-0003-v7.4

Status: Ratified
Document type: Policy

Contents

1 Introduction

Under the Data Protection Act 2018 (GDPR), legally enforceable standards apply to the collection and processing of images relating to individuals.

The Information Commissioner has published a CCTV Code of Practice which sets out the measures which must be adopted to comply with the Data Protection Act 2018 (GDPR).

If CCTV shows a recognisable person then it is generally classed as Personal Data and is covered by the Data Protection Act.

Anyone who believes they have been filmed by CCTV is entitled to ask for a copy of the images, subject to the exemptions on access under the Act.

2 Why we need this policy

2.1 Purpose

This document sets out the actions and procedures which must be followed to comply with the Data Protection Act 2018 (GDPR) in respect of the use of CCTV (closed circuit television) camera surveillance where it is installed in Tees, Esk and Wear Valleys NHS Foundation Trust locations.

2.2 Objectives

By adhering to this policy, the Trust can ensure that CCTV cameras throughout the Trust will be installed and used in compliance with the principles of:

- Data Protection Act 2018 (GDPR),
- Human Rights Act 1998,
- Regulation and Investigatory Powers Act 2000

and other UK and EEA relevant legislation.

3 Scope

This policy covers the use of the following types of system:

- Video
- Digital on PC
- Real time viewing

Where relevant, the operation of each type of system is covered in the topics below.

The Regulation of Investigatory Powers Act 2000 regulates the use of covert/directed surveillance and is subject to a strict code of practice.

Use of CCTV in these circumstances or for any other reason other than that authorised in accordance with this policy is not covered by this policy and in such circumstances further guidance should be sought from the IG and Records department.

3.1 Who this policy applies to

This policy applies to all staff within TEWV and others working on behalf of the Trust.

3.2 Roles and responsibilities

Role	Responsibility
Trust Board / Relevant executive director	Implementation of policy, monitoring its effectiveness and ensuring the CCTV policy is available to staff and the general public for reference purposes.
Head of Information Governance	Ensures that the Trust's use of CCTV Systems is registered with the Information Commissioner under the terms of the Data Protection Act 2018 (GDPR) Ensures that the policy and Code of Practice are adhered to and monitors this compliance. Responds to complaints relating to processing under the Data Protection Act. Responds to Subject Access Requests in accordance with Data Protection legislation.
Local Managers	Oversee the monitoring of all images in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with written operational procedure Information Asset Owners will act as the data controller and are responsible for: • Updating asset registers so that all areas undertake their responsibilities and communicate with others where necessary: • Establishment of repair and maintenance contracts • Checking Information Security if access to the Trust network is required • Ensuring that new systems are linked to a Trust manager for overall oversight • Following this policy and producing local protocols for the use of CCTV Systems within their area of control. • Responding to Subject Access Requests in accordance with Trust policy.
Information Security officer	Ensures local procedures cover all requirements of the Act and staff are allocated and trained to preserve, copy and store forensic evidence in all reportable incidents.

Estates department	Maintain a register of locations containing repair and maintenance contracts for CCTV. This is not Trust wide and does not include CCTV in PFI sites.
Local Security Management Specialist	Ensures that all Trust locations have adequate signage in multiple locations to inform members of the public that CCTV is in operation, and details of who to contact in the event of a request or further information.

4 Policy

4.1 General Principles

All schemes will operate in accordance with the guidelines set out in the "CCTV Code of Practice" published by the Office of the Information Commissioner, a copy of which is available from the Trust Data Protection Co-ordinator or direct from the Information Commissioner's website.

Cameras will not be hidden from view and we will inform the public of the presence of the system and its ownership at all times

CCTV cameras within the Trust will not be used for covert surveillance unless authorized.

There will be no sound recording undertaken from any part of the system.

Images from the cameras are appropriately recorded in accordance with existing operational procedures (see Appendix 4).

4.2 Before installation

All covert surveillance undertaken by NHS bodies must have appropriate authorisation. Any requests for covert surveillance must be made through the Trust's Local Security Management Specialist (LSMS), Information Security Officer or the Head of Information Governance and Records Management.

This will ensure that the operation is carried out in accordance with all applicable laws and is subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenges under the Human Rights Act 1998.

4.2.1 Initial Assessment Procedures

Under the Data Protection Act, CCTV may be used to:

- Support Police in a bid to prevent or detect crime or disorder;
- Assist in the identification, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings);

- increase personal staff/patient/public safety and reduce fear of crime;
- Protect the premises and their assets.

Prior to any camera installation the LSMS, Information Security Officer and local site manager will be able to assist and advise to ensure that the installation complies with the complies with the Data Protection Act and CCTV Code of Practice, thereby ensuring privacy by design. This will involve the Information Security Officer undertaking a Data Protection Impact Assessment.

Each installation must be supported by a scheme which details the rationale for the CCTV requirement.

4.3 Installation

4.3.1 Siting the Cameras

All cameras are located in prominent positions within public and staff view.

The location of the equipment must be carefully considered, because the way in which images are captured will need to comply with the Data Protection Act.

To ensure privacy, cameras will operate so that they only capture images relevant to the purpose for which that particular scheme has been established and approved.

Signage will be placed on all entrance points to Trust premises to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signage must include details of the purpose, organisation and contact details; see example in Appendix 1.

Upon installation, all equipment must be tested to ensure that only the designated areas are monitored and clear high quality pictures are available in live and play back mode.

4.3.2 Specification

It is important that the images produced by the equipment are as clear as possible so they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified; for example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

Only companies approved by organisations such as the National Security Inspectorate (NSI) and the Security Systems and Alarms Inspectorate Board (SSAIB) will be used to supply and install CCTV systems.

4.3.3 Training

The Trust provides training programmes for Trust staff on the Data Protection Act and CCTV Code of Practice.

4.4 Maintenance

All schemes will be administered by the local manager who will be identified and named prior to the scheme going live.

The local manager is responsible for ensuring that:

- Cameras are properly maintained and serviced to ensure that clear images are recorded.
- Any new maintenance contracts will need to be arranged with the Estates Department
- Recording maintenance.
- If a time/date facility is used on the system, regularly checking to make sure that the system is displaying the correct time and date.

All faulty equipment within the CCTV system that could affect picture or recording quality should be repaired or replaced as soon as practically possible

Failure to repair faulty equipment not only compromises the efficacy of the system, but also breaches two of the regulations of the Data Protection Act 2018 (GDPR) – that data should be adequate and accurate (Article 5(c) and (d)).

4.5 Retention and Processing of images

Images which are not required for the purpose(s) for which the equipment is being used should not be retained for longer than is necessary.

Retention periods will be defined in local protocols and based on local requirements. Images are routinely deleted by being overwritten unless the image is required for evidential purposes then it must be separately retained.

While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 2018 Act.

- Hard copies (discs, video tapes) of images must be securely stored within a locked cabinet for the retention period. Once this period has expired, the image will be erased.
- To maintain image quality, tapes should be used no more than 12 times i.e. once a month for a year.
- Sub monitors are located in the Trust for real time viewing which display images of public areas; they must be enclosed in secure areas and only be accessible to Trust staff.

Where CCTV images are required for evidential purposes in legal or Trust disciplinary proceedings, they will be properly processed following consultation with the Head of Information Governance and Data Protection and the Information Governance Manager.

The recording will be placed in a sealed envelope which is signed, dated and then stored securely until the investigation is complete. Viewing of images is controlled by the Local Manager or a person nominated to act on his behalf.

Tapes or images will not be made available to the media, for commercial gain or entertainment.

4.6 Access to and disclosure of images to third parties

Access to and disclosure of images is permitted only if it supports the purpose of the agreed scheme. Under these conditions the video/data record book and the appropriate image release form, Appendix 2, must be completed.

Access to CCTV images is restricted to authorised Trust staff and third parties as detailed in the purpose of the scheme.

Images may also be made available to the Police/Crown Prosecution Service/Solicitor/ NHS Legal Protection Unit where requests are made under section 29 of the Data Protection Act for the purpose of detecting crime.

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled. This will ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes e.g., a Police enquiry or an investigation being under taken as part of the Trust's disciplinary procedure.

Advice on any of these issues can be sought from the Information Governance department (tewv.informationgovernance@nhs.net).

5 Access to images by individuals

Article 15 of the Data Protection Act 2018 (GDPR) gives any individual the right to request access to CCTV images.

A person whose image has been recorded and wishes to access the tape must make a formal written request to the Data Protection Officer who can validate the request. If insufficient detail is given to process the request, requesters will be issued a copy of the subject access request form, Appendix 3. If all info not available, will seek clarification through SAR form

Please refer to the Request for Information procedure.

In addition to being given access to the images, individuals must be provided with a description of any recipients of the data, the purposes for which the data is used and the source of the information. In the case of CCTV this will include providing information on camera locations.

Where 3rd party data is provided on a CCTV tape, the local manager must decide:

- whether to disclose without disguising the features of 3rd parties.
- Where a decision is made **not** to release information identifying 3rd party data, the images must be edited so that they obscure the faces of any identifiable 3rd parties.

Depending upon the type of CCTV equipment used, specialist companies may be required to perform this work; advice can be sought from the Trust's Information Security Officer.

Any requests received for the disclosure of information under the Freedom of Information Act 2000 will be directed to the Trust Secretary in the first instance. The request will be considered within the strict guidelines of the Act.

5.1 Education and training

The Trust reserves the right to use CCTV footage where appropriate to debrief teams following an incident.

If the incident has wider Trust relevance in terms of lessons learned, the CCTV footage will be anonymised before being shared as training tool.

5.2 Complaints

Formal complaints received in relation to the CCTV scheme will be managed through the Trust's complaints process with assistance from the local manager of the unit and advice from the Information Governance Team.

Complaints received about processing under the Data Protection Act will be dealt with by the Head of Information Governance and Records. Where these cannot be resolved, the individual has the right to escalate the complaint to the office of the Information Commissioner.

5.3 Documentation

Copies of all documentation and records relating to the CCTV scheme will be held by the Trust's Information Governance and Records team and will be kept, under restricted confidentiality, for a period of 6 years from disestablishment of the CCTV system.

6 Definitions

Term	Definition
Sensitive personal data'	images of individuals stored either digitally or on video tape

7 Related documents

Access to Information Procedure
Freedom of Information procedure
CCTV procedure

8 How this policy will be implemented

- Guidance in the requirements of the law on Data Protection will be given to staff who are required to manage and work the CCTV systems
- Staff will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation.
- Local training will be given in procedure and process due to the range of equipment in use within the Trust.

• This policy will be published on the Trust's intranet and external website.
• Line managers will disseminate this policy to all Trust employees through a line management briefing.

9 How this policy will be audited

IG Liaison Spot checks incorporate include assessment of external (and, where applicable, internal) signage; the Trust's Internal Auditors, Audit North will undertake all other required reviews.

10 References

Data Protection Act 2018 (GDPR), HMSO
CCTV Code of Practice 2000, Information Commissioner
NHS Security Management Services Security Manual Section 5 (CCTV)
Human Rights Act, HMSO
Regulation and Investigatory Powers Act 2000
Records Lifecycle Policy
Privacy and Electronic Communications Regulations

10.1 Appendix 1 - Example CCTV poster

CCTV

Images are being monitored for the purposes of crime prevention and patient, staff and public safety.

This scheme is controlled by

Tees, Esk and Wear Valleys
NHS Foundation Trust

For further information about the scheme please contact ……

10.2 Appendix 2 – Release form for a CCTV Image

RELEASE FORM FOR A CCTV IMAGE

Declaration: I understand that any information I obtain from recording medium is protected under the Data Protection Act 2018 (GDPR).

Details of Person Releasing the Image
Print Full Name ……Position ……..…….
Signature ……..Date the Image was released ……...

Details of Person Requesting Image Viewing
Print Full Name ……Position ……..……..……....
Signature ……..……PC Number (if Constabulary) ……....

The reason for releasing the image

☐ Preventing or detecting crime or disorder

☐ Apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings)

☐ Interest of public and employee safety

☐ Protecting public health

☐ Staff disciplinary investigations

Reasons ……..…….
……..
……..

Date and times of Image to be released.…….……
Camera Number to be released……...

10.3 Appendix 3 – Request to Access CCTV Image

CCTV Image Request Form

DATA PROTECTION ACT 2018 (GDPR)

REQUEST FORM FOR ACCESS TO CCTV IMAGES

Under the Data Protection Act 2018 (GDPR), you have the right to inquire of any organisation whether they hold your personal data and see a copy of that information.

Please complete this form and return together with the necessary verification details if you wish to have access to your record. **On completion this form should be returned to the *Data Protection Team, Medical Records, Lanchester Road Hospital, Lanchester Road, Durham DH1 5RD*. A response will be provided within 30 days of receipt of the completed form and proof of identity.**

Declaration: I understand that any information I obtain from a tape is protected under the Data Protection Act 2018 (GDPR).

Details of Person Requesting Access

Print Full Name ……Position ……..……

Signature ……..……Address……..…….

…….Contact number ……..……...

Date completed ……./……./…….

The reason for access:

……..……

……

……

Brief description of the applicant's appearance and likely activities captured by CCTV

……...

……

……

Date and times of Image to be viewed ……..……

Location / Camera Number to be viewed ……..

Type of access required: Viewing ☐

Copy of image ☐

Other ☐

Please return this form together with the administration fee, with proof of identity such as passport, driving licence or utility bill showing name address dated within last 3 months.

Item 1 (e.g. passport)

Item 2
For Data Protection Officer Use Only

Date request received ……/……/…….

Details of Person who will supervise the Access
Print Full Name ……Position (PC No.) …….
Signature ……..Date the Image was viewed ……

Details of Person who assessed the request of Access

Print Full Name ……Position ……

Signature ……..Date……..

Access approved ☐ **Access not approved** ☐

Reasons ……..……..
……

11 Document control

Date of approval:	10 October 2018	
Next review date:	10 April 2022	
This document replaces:	CORP-0003-v7.3 CCTV Policy	
Lead:	Name	Title
	Lynn Jackson	Information Security Officer
Members of working party:	Name	Title
	GDPR Steering Group	
This document has been agreed and accepted by: (Director)	Name	Title
	Patrick McGahon	Director of Finance and Information
This document was approved by:	Name of committee/group	Date
	Digital Safety and Information Governance Board	03 October 2018
This document was ratified by:	Name of committee/group	Date
	Executive Management Team	10 October 2018
An equality analysis was completed on this document on:	22 March 2016 CORP-0003-v7.3 EA CCTV Policy.pdf	

Change record

Version	Date	Amendment details	Status
7(2)	1 Oct 2013		Obsolete
7.3	6 Apr 2016	Amended to reflect need for Local CCTV Procedures	Obsolete
7.4	13 Jun 2018	Minor amendments to reflect Data Protection Act 2018 (GDPR)	Published
7.4	Oct 2020	Review date extended to 10 April 2022.	Published