



Public – To be published on the Trust external website

CCTV Policy

CORP-0003-v8

Status: Ratified

Document type: Policy



Last amended: 18 May 2022

1	Introduction	3		
2	Why we need this policy	3		
2.1	Purpose	3		
2.2	Objectives	3		
3	Scope	4		
3.1	Who this policy applies to	4		
3.2	Roles and responsibilities			
4	Policy			
4.1	General Principles	5		
4.2	Before installation	6		
4.2.1	Initial Assessment Procedures	6		
4.3	Installation	6		
4.4	Training	7		
4.5	Maintenance	7		
4.6	Retention and Processing of images	7		
4.7	Access to and disclosure of images to third parties	8		
5	Access to images by individuals	9		
5.1	Education and training	9		
5.2	Complaints	10		
5.3	Litigation	10		
5.4	Documentation	10		
6	Definitions	10		
7	Related documents	10		
8	How this policy will be implemented			
3.1	Implementation action plan	11		
3.2	Training needs analysis	12		
9	How the implementation of this policy will be monitored			
10	References			
11	Document control (external)	13		
Appendix 1 - Example CCTV poster and signage14				
Appendix 2 – Release form for a CCTV Image16				
Appendix 3 – Request to Access CCTV Image17				
Appendix 4 - Equality Analysis Screening Form19				
Appendix 5 – Approval checklist				





1 Introduction

Under the Data Protection Act 2018, 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 (DPA 2018).

If CCTV shows a recognisable person then it is generally classed as Personal Data and is covered by the DPA 2018.



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 DPA 2018.

Our Journey To Change sets out why we do what we do, the kind of organisation we want to become and the way we will get there by living our values, all of the time. To achieve this, we have committed to three goals.

This policy supports the Trust's first strategic goal of co-creating a great experience for patients, carers and families, as they can be assured that their images captured via CCTV, and their rights as data subjects, are being managed lawfully (Data Protection Act 2018).

The policy also supports the second goal of co-creating a great experience for staff by providing colleagues with the knowledge and tools to ensure they are managing CCTV images in a way that keeps them safe and within the law.

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 DPA 2018 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,
- Human Rights Act 1998,
- Regulation and Investigatory Powers Act 2000 and other UK and EEA relevant legislation.





Last amended: 18 May 2022

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.

This policy does not apply to footage captured by the patient monitoring system Oxehealth – refer to the Oxehealth Standard Operating Procedure.



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 who has responsibility for managing and processing CCTV recordings and equipment.

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 DPA 2018	
	Ensures that the policy and Code of Practice are adhered to and monitors this compliance.	
	 Responds to complaints relating to processing under the DPA 2018. 	
	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, destruct and maintenance of all storage media is conducted in accordant with written operational procedure	





Last amended: 18 May 2022

	 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.
Senior 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
	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 Information Commissioner's website.



Cameras will not be hidden from view and we will inform patients and the public of the presence of the system and its ownership at all times through signage and our privacy notices.



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

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), Senior Information Security Officer or the Head of Information Governance.

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.

Before any camera installation the LSMS, Senior 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 DPA 2018 and CCTV Code of Practice, thereby ensuring privacy by design. This will involve the Estates Officer who is responsible for the installation completing a Data Protection Impact Assessment.



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

4.3 Installation



All cameras are located in prominent positions within patient, 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 DPA 2018.

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.





Last amended: 18 May 2022

The images produced by the equipment must be as clear as possible so they are effective for their intended purpose(s).

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.

4.4 Training

The Trust can provide training for Trust staff on the DPA 2018 and CCTV Code of Practice.

4.5 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 will 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 – that data should be adequate and accurate (Article 5(c) and (d)).

4.6 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 the local installation. 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 DPA 2018.





Hard copies (discs, video tapes, USB memory sticks) of images must be securely stored within a locked cabinet for the retention period. CCTV recordings will be retained in accordance with the NHSX Records Management Code of Practice 2021 retention scheduled based on the purpose for which the footage was captured. 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.



Within all services, when a Serious Incident is known or suspected it is imperative that if CCTV is known to be active in the area concerned, that the images are harvested and retained to enable a full investigation to take place.

In the event that the incident is not viewed on CCTV imagery, the footage MUST still be harvested and retained to provide the evidence that the incident in question did not take place.

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 their behalf. A log will be kept of who has accessed footage (see CCTV Procedure for more information).

CCTV cameras are not placed in bedrooms. If CCTV images capture a patient in a state of undress, the exposed body parts will be pixelated where necessary unless relevant to the circumstances of the request for the footage.



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

4.7 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 be made available to the Police/Crown Prosecution Service/Solicitor/ NHS Legal Protection Unit where requests are made under the DPA 2018 for the purpose of detecting crime. Images may also be shared with professional bodies where allegation of professional misconduct is being investigated.

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

Ref: CORP-0003-v8 Page 8 of 23 Ratified date: 18 May 2022 CCTV Policy Last amended: 18 May 2022





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 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 (SAR) form, Appendix 3. If all info not available, will seek clarification through SAR form. If a verbal request is made, the person will be directed to the 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 if there is a legal duty to do so.
- 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.

In the event that 3rd party images are shared, the local manager will advise the 3rd party that this is going to take place.

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. Within the claims process, CCTV footage is not disclosed without a Court Order as any patient images cannot be pixilated.

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.





Last amended: 18 May 2022

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 DPA 2018 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 Litigation

As litigation can be pursued against the Trust, any CCTV footage viewed for any reason or involved in an investigation process should be preserved and retained for a period of three years from the date of the incident. This is to enable the Claims and Legal Services Manager to request a copy of the footage in order to comply with the Pre-Action Protocols of the Civil Procedure Rules of which there is a duty to preserve disclosure documents and other evidence such as CCTV. If documentation is destroyed this could be seen as an abuse of the court process.

5.4 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.

The Claims and Legal Services Manager also keeps documentation and records relating to claims and CCTV separately from the above process.

6 Definitions

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

7 Related documents

- Access to Information Procedure
- CCTV procedure

8 How this policy will be implemented





Last amended: 18 May 2022

- 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.

8.1 Implementation action plan

Activity	Expected outcome	Timescale	Responsibility	Means of verification/ measurement
Development of local protocol	Local protocol in place at each site where CCTV is installed	3 months	Modern Matron / Ward Manager / Team Manager	Local CCTV protocol available





Last amended: 18 May 2022

8.2 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
Staff working on sites where CCTV is installed	DPA 2018 and CCTV requirements	50 minutes	Once
Staff responsible for retrieving CCTV images	CCTV operation	Duration is dependent upon the particular installation	Once

9 How the implementation of this policy will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Completion of subject access request (SAR) within legal timescales	Monthly SAR reporting by Information Governance Manager	Information Management Meeting

10 References

Data Protection Act 2018, 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





Last amended: 18 May 2022

11 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	18 May 2022 (pending)
Next review date	18 May 2025
This document replaces	CORP-0003-v7.3 CCTV Policy
This document was approved by	Digital Performance and assurance Group
This document was approved	06 April 2022
This document was ratified by	Management Group
This document was ratified	18 May 2022
An equality analysis was completed on this policy on	14 January 2022
Document type	Public
FOI Clause (Private documents only)	N/A

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	Obsolete
8	18 May 2022	Our Journey to Change wording added to introduction.	Published
		4.3.2 para added re connection to network or use of encrypted USB storage devices	
		4.5 blue box added re retention of CCTV in relation to serious incidents	
		Section 5 sentence added re verbal requests. Also sentence that CCTV about patients is not released without a court order.	
		5.3 added re retention of CCTV in relation to litigation	
		Minor amendments throughout	





Last amended: 18 May 2022

Appendix 1 - Example CCTV poster and signage

CCTV

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

This scheme is controlled by



For	further	information	about the	scheme	please
cor	ıtact				





IMAGES ARE BEING MONITORED AND RECORDED FOR THE PURPOSE OF CRIME PREVENTION AND FOR THE SAFETY OF THE PUBLIC

THIS SCHEME IS BEING OPERATED BY

TEES, ESK AND WEAR VALLEYS NHS FOUNDATION TRUST

0191 333 6637





Last amended: 18 May 2022

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.

Details of Per	son Releasing the Image				
Print Full NamePosition					
Signature	SignatureDate the Image was released				
Details of Per	son Requesting Image Viewing				
Print Full Nam	nePosition				
Signature	PC Number (if Constabulary)				
The reason f	or 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-related investigations				
Reasons					
Date and time	es of Image to be released				
Camera Num	ber to be released				





Appendix 3 - Request to Access CCTV Image

CCTV Image Request Form

DATA PROTECTION ACT 2018 REQUEST FORM FOR ACCESS TO CCTV IMAGES

Under the Data Protection Act 2018, 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 <u>Data Protection</u> <u>Team, Medical Records, Lanchester Road Hospital, Lanchester Road, Durham DH1 5RD</u>. 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.

Details of Person Requesting Access Print Full Name			
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: View	ving		
Copy of	image		
Oth	er		





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 NamePosition (PC No.)			
SignatureDate the Image was viewed			
Details of Person who assessed the request of Access			
Print Full NamePosition			
SignatureDate			
Access approved Access not approved			
Reasons			

Ratified date: 18 May 2022 Last amended: 18 May 2022





Appendix 4 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Digital and Data Services
Title	CCTV Procedure
Туре	Procedure
Geographical area covered	Trust-wide
Aims and objectives	To give guidance within all locations as to the preservation and duplication of CCTV images within legal guidelines.
Start date of Equality Analysis Screening	June 2020
End date of Equality Analysis Screening	14 January 2022

Section 2	Impacts		
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	All persons requesting CCTV images for all areas within the Trust, ensuring that all imaging is harvested and duplicated correctly and in line with the Data Protection Act 2018.		
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	 Race (including Gypsy and Traveller) NO Disability (includes physical, learning, mental health, sensory and medical disabilities) NO Sex (Men, women and gender neutral etc.) NO Gender reassignment (Transgender and gender identity) NO Sexual Orientation (Lesbian, Gay, Bisexual and Heterosexual etc.) NO Age (includes, young people, older people – people of all ages) NO Religion or Belief (includes faith groups, atheism and philosophical beliefs) 		





	 Pregnancy and Maternity (includes pregnancy, women who are breastfeeding and women on maternity leave) NO Marriage and Civil Partnership (includes opposite and same sex couples who are married or civil partners) NO 	
Describe any negative impacts	None identified	
Describe any positive impacts	The procedure provides assurance that all requests for CCTV footage will be handled with equal importance and in line with legislation and best practice.	

Section 3	Research and involvement
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	Data Protection Act 2018 Information Commissioners Office best practice guidelines
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	Yes
If you answered Yes above, describe the engagement and involvement that has taken place	The CCTV policy which this procedure sits under and this procedure have been out for Trust-wide consultation. Trust staff comprise all protected characteristics.
If you answered No above, describe future plans that you may have to engage and involve people from different groups	N/A

Section 4	Training needs
As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A

Ratified date: 18 May 2022 Last amended: 18 May 2022





Last amended: 18 May 2022

Describe any training needs for contractors or other outside agencies

Check the information you have provided and ensure additional evidence can be provided if asked



Appendix 5 – Approval checklist

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	Title		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	Rationale		
	Are reasons for development of the document stated?	Yes	
3.	Development Process		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	Content		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	Evidence Base		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	Training		
	Have training needs been considered?	Yes	
	Are training needs included in the document?	Yes	
7.	Implementation and monitoring		
	Does the document identify how it will be implemented and monitored?	Yes	
8.	Equality analysis		

Page 22 of 23

Ratified date: 18 May 2022 Last amended: 18 May 2022

	110	_	4.4	-
N	н۷	Found	ation	Iruct

	Title of document being reviewed:	Yes / No / Not applicable	Comments
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	14 January 2022
9.	Approval		
	Does the document identify which committee/group will approve it?	Yes	
10.	Publication		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	Yes	