Public – To be published on the Trust external website

# Procedure for the monitoring, saving and harvesting of CCTV images

# Ref: CORP-0003-001-v3

**Status: Approved**
**Document type: Procedure**

## Contents

**1 Purpose ..... 3**
**2 Related documents ..... 3**
**3 CCTV procedure ..... 4**
3.1 Who wants it? ..... 4
3.2 When do they need it? ..... 4
3.3 What do they need? ..... 5
3.4 Who will do it? ..... 5
**4 Local CCTV protocol ..... 6**
**5 Terms and definitions ..... 6**
**6 Document control (external) ..... 7**

Appendix 1 – Surrender of stored imagery to Police ..... 8
Appendix 2 – Imagery viewing by external agencies ..... 9
Appendix 3 –Data Protection Act 2018 guidance for staff ..... 10
Appendix 4 – Data Protection Act 2018 request form for access to CCTV images ..... 12
Appendix 5 – Process for retrieval of footage when the system will not accept an encrypted USB stick ..... 14
Appendix 6 - Equality Analysis Screening Form ..... 15
Appendix 7 – Approval checklist ..... 18

# 1 Purpose

Following this procedure will help the Trust to:-

- Meet all legal requirements in the monitoring, saving and harvesting of CCTV images from applicable Trust locations in accordance with the Trusts CCTV policy.
- Allow specific local procedure documents to be manufactured in accordance with the overall requirements procedure itself by providing the guidelines needed to suit the differing types of technology which are used throughout the Trust locations and the divergent staff who will need to follow the procedure.

This procedure does not apply to footage captured via the patient monitoring system Oxehealth – refer to the Oxehealth Procedure.

Each location where CCTV is in place must develop their own local protocol which specifies the requirements for monitoring, saving and harvesting CCTV images on that individual site.

# 2 Related documents

This procedure describes what you need to do to implement the 5.6 section of the CCTV Policy.

This procedure also refers to:-

- Information, Security and Risk Policy
- Email Policy

# 3 CCTV procedure

The images collected and stored on the site's CCTV system may need to be reviewed for a number of reasons. These include issues regarding the safety of patients, staff and visitors to the hospital, damaged or missing property, details of patients who go missing from the hospital and reviewing serious incidents or clinical practice.

Whenever a Serious Incident has or is suspected to have taken place, CCTV must be harvested for review (see 3.4 – Who will do it)

A copy must be made and secured as evidence on the team shared drive. This ensures that, whether an incident occurred or not, the footage is available for review.

All copies made for this purpose must be undertaken with two persons present; one to harvest the images, and one to witness the procedure to ensure nothing is missed or accidentally amended.

Follow this naming convention to ensure the saved footage is easily located:

[YYYY_MM_DD HHMM Paris ID]

e.g. 2019_10_31 2048 123456

Multiple Paris IDs may be needed if more than one patient is included in the footage.

Whenever a review of CCTV coverage is required a number of considerations must be made.

## 3.1 Who wants it?

Requests to review CCTV images may come from a number of sources including investigating officers including those acting on behalf of professional bodies, clinical areas, safeguarding teams, Health, Safety and security team and the police. Permission to review CCTV coverage should be given at locality manager level (or nominated deputy i.e. Manager on-call) before any review takes place.

## 3.2 When do they need it?

Whenever possible the reviewing of CCTV coverage should be carried out by management staff (Band 7 or above) however the nature of the incident to be reviewed may mean that this needs to be done immediately, when there are no Band 7 staff available. The decision of whether immediate review is required will be made by the locality manager (or nominated deputy), if this is the case then Band 6 staff will be expected to review the appropriate coverage. Paper copies (i.e. a screen shot which is captured then printed out) of CCTV coverage are available but can only be obtained by staff of Band 7 or above. If paper copies of CCTV coverage are required then this must only be done with the express permission of the IAO - Information Asset Owner (or nominated deputy, usually the IAA - Information Asset Administrator) and produced whenever a Band 7 (or above) member of staff is available to do so.

## 3.3 What do they need?

Before any review of CCTV coverage can take place a clear outline of what information is required needs to be made, the approximate time range of the review and the areas of the hospital that are of interest.

Where a review of the CCTV coverage needs to take place in collaboration with outside agencies, authorisation from the IAO (or nominated deputy, usually the IAA will be required before this joint review can take place and the imagery viewing by external agencies form completed [See Appendix 2] All Trust locations must use this form; any other forms will be rejected.

The police may require copies of CCTV coverage as evidence in any investigation they undertake. In such cases the police should make a request under the Data Protection Act. An exception to this is when the Trust has asked the police for assistance in investigating an incident, in which case no personal data access request form is required. See Appendix 3 for more details.

Copies of CCTV coverage and these should only be provided with the authorisation of the Head of Service and the completion of the Surrender of Stored imagery to the Police form [Appendix 1]

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. Verbal requests can also be made in which case the person will be directed to complete the request form. Individuals who request access to images must be issued a copy of the subject access request form, [Appendix 4].

## 3.4 Who will do it?

The reviewing of CCTV coverage has 5 main elements:

1) Logging onto the system, identifying the correct camera coverage at the requested time.
*This process will be completed by the appropriate nominated person following the correct identified training.*

2) Reviewing of the CCTV coverage, noting the exact time and camera of all reviewed coverage.
*This will be carried out by Trust staff of Band 6 (or above) in conjunction with the person requesting the information. See section "3.2* When do they need it?" *for authorisation guidance.*

3) Any reviewed coverage must be saved into a restricted-access folder of the team/unit shared drive in order to evidence that the situation has been reviewed, regardless of whether anything significant has been determined.
*The reviewing member of staff will record details of all coverage that has been reviewed (camera number, times etc.) and provide this information to the locality manager who will make arrangements for the coverage to be securely saved onto the system.*

4) Copies of coverage may be required. The preferred methodology for this activity is via secure email (Egress) in line with guidance provided in the Email Policy or if you are

disclosing to the Police you may be requested to use the NICE portal. Further guidance or clarification can be sought by contacting the TEWV.InformationCompliance@nhs.net

*Copies of coverage must be downloaded and produced by a Band 7 (or above) member of staff who has completed the necessary training to do so. If the system does not enable an encrypted USB stick to be used, follow the process in Appendix 5. If the footage being saved is a primary document e.g. for an investigation or as a disclosure to the police, both copies will be kept and have a retention schedule applied depending on the purpose/activity. A copy that is kept for information only will be a secondary copy and deleted when no longer required.*

5) Keeping a record of the request.

*Each site where CCTV equipment is located will develop their own local CCTV protocol which includes the process for logging CCTV requests (see section 4 below)*

# 4 Local CCTV protocol

Each site where CCTV is used must develop their own local:

- CCTV protocol
- CCTV requests log
- CCTV action card

This is because CCTV systems and responsibility for accessing and retrieving footage vary from site to site. Staff need to know who to contact and any additional requirements for their area such as use of a USB stick.

- Click here for the Local CCTV Protocol Template
- Click here for the CCTV request log template
- Click here for the blank CCTV action card

# 5 Terms and definitions

| Term | Definition |
|---|---|
| CCTV | • Closed Circuit Television |
| IAO | • Information Asset Owner |
| IAA | • Information Asset Administrator |
| Egress | • The approved methodology for sending large files to other organisations via NHS email |

# 6 Document control (external)

To be recorded on the policy register by Policy Coordinator

| | |
|---|---|
| Date of approval | 13 March 2026 |
| Next review date | 13 March 2029 |
| This document replaces | CORP-0003-001-v2 CCTV Procedure |
| This document was approved | Information Governance Group (IGG)<br>17 December 2025 |
| This document was approved | Data Protection Assurance Group (DPAG) (virtual)<br>13 March 2026 |
| 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 |
|---|---|---|---|
| 1 | 20 Jul 2016 | New document | Withdrawn |
| 1.1 | 14 Aug 2019 | Minor amendments in line with Data Protection Act 2018 | Withdrawn |
| 2 | 15 Mar 2022 | Section 3 – blue box added re retrieval of images in relation to serious incidents. Section 4 added re local CCTV protocol. Appendix 5 process added for use of USBs. Minor updates throughout | Withdrawn |
| 2 | Feb 2025 | Review date extended from 15 March 2025 to 31 October 2025 | Withdrawn |
| 3 | 13 Mar 2026 | Updated: Information Compliance Manager & Acting DPO - Minor updates with references to appropriate appendix<br>Updated with email address of Access Team<br>Information removed which references the use of DVD and USB for data transfer.<br>Information added regarding the use of the NICE portal for the sharing of images with the police only | Published |

## Appendix 1 – Surrender of stored imagery to Police

### SURRENDER OF STORED IMAGERY TO POLICE

**In the event that stored imagery is required for evidential or investigation purposes, advance permission is required from the Clinical Director and the Head of Service.**

**I (signature)_____ being one of the above-**

**named, authorise release of stored imagery,**

**Date/Time/Location_____**

**_____**

**to the police on _____(date).**

**The receiving Police Officer is required to provide the following confirmation of receipt of footage:**

**I (signature / name) _____ being a**

**Police Officer, warrant card number_____**

**Assigned to _____Police Station,**

**Acknowledge receipt of footage, (Date/Time)_____**

**On _____(date) from**

**_____(Site) for the**

**Purpose of investigation with regard to Incident index number_____**

(Alternatively if the request is being facilitated via the NICE portal appropriate reference numbers, dates and times should be recorded for assurance purposes)

## Appendix 2 – Imagery viewing by external agencies

### IMAGERY VIEWING BY EXTERNAL ACENCIES

**In the event that stored imagery needs to be viewed immediately by an external agency for the prevention, detection or investigation of a crime or incident, advance permission is required from the Clinical Director, Head of Service (or nominated deputy).**

**Name _____ representing one of the above**

**named, authorise the immediate viewing of footage,**

**Date/Time/Location_____**

**_____**

**by the external agency on _____(date).**

**The viewing representative of the viewing agency is required to sign for receipt below:**

**I (signature)_____**

**from (name of agency) _____**

**Acknowledge viewing of footage on site, on _____(date)**

**for the Purpose of investigation with regard to**

**Incident reference number_____**

# Appendix 3 –Data Protection Act 2018 guidance for staff

## DATA PROTECTION ACT 2018 GUIDANCE FOR STAFF

Article 15 of the Data Protection Act 2018 is the section of the Act used by the Police to request information from the trust which we would normally withhold. It is the exemption which makes it possible for Police to request any information from us for the detection and prevention of crime, or for the purposes of solving a crime.

***When we ask the police for assistance:***

We may ask the police for help with numerous things, from patients absconding to assaults on staff and from break-ins to trust locations to accidents in car parks. When we are requesting help, we can give any information we think is necessary for the police to have in order to help us WITHOUT A PERSONAL DATA ACCESS REQUEST FORM, as it is the trust who is asking for aid.

***When the police ask us for assistance:***

If the Police ask us for copies of records or CCTV, or any personal identifiable information for any reason (other than a trust request for assistance) then a personal data access request form is required. This is to ensure that the Police have a justification for requesting copies of that information. It also ensures that we do not give the police items of information which they do not need to know for that particular case or person. For example, if a personal data access request was made for a copy of the complete records, we would ask for specific dates rather than give them a copy of everything: they may not be aware that the person has been engaging in service since a young age, and they are only looking for an event in the past five or so years.

A personal data access request form should be completed for every request by the police to the trust (unless the trust has requested help) and will state the requestors name, rank and number and will be countersigned by an Inspector (at least) with name rank and number. It will also state the justification for the request and should also give the required timelines. This request is dealt with in the same way as a Data Protection Subject Access Request, but is done as soon as possible to aid detection. There is no time limit for a personal data access request, but best endeavours usually ensure that the request is fulfilled in a matter of hours or days.

***Article 15 and CCTV***

***When we ask the police for assistance:***

If the trust is asking for police help with, for example, an assault on a member of staff in a corridor by a member of the public, then the footage should be given to the police using secure email (Egress). Alternatively police may request the disclosure of information via the NICE or secure email.

As something like this could be cause for litigation against the trust, the footage should be duplicated and retained securely in an appropriate folder on the unit's / service's shared drive for a period of three years. This is to enable the Trust Solicitor to request a copy of the footage in the legal period in which a person can legitimately make a claim against the trust.

***When the police ask us for assistance:***

The trust may also get requests for CCTV on a personal data access request form. This is usually more explicit, as the police may be looking for a certain person who may have been on our premises on a specific date around an agreed time. In this case, the police may only want to view the CCTV footage, or they may request a copy of the footage to take back to police Headquarters for further viewing.

If the request is view only, arrangements will be made between the police and the manager who is administrating the CCTV for the police to view the footage in a secure area, away from others and where the monitor cannot be overlooked.

If the request is for a copy of the footage, this will be done under the local procedures in place at that location. The administrator of that system will cut the footage and check it has been copied correctly. They will then fill in the request form in the local procedures paperwork to provide an appropriate audit trail.

# Appendix 4 – Data Protection Act 2018 request form for access to CCTV images

**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 *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**

**This form can also be submitted electronically to:**
**TEAWVNT.AccessRequests@nhs.net .**

**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 ……Position ……..……

Signature ……..……

Address……..……. …….…..…….

Contact number ……..……...

Date completed ……./……./…….

**The reason for access request:**

……..…….……

……

……

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, 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 Team Use Only**

Date request received ……/……/……..

Details of Person who will supervise the Access

Print Full Name ……Position ……

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 ……..……..

……

## Appendix 5 – Process for retrieval of footage when the system will not accept an encrypted USB stick

Unencrypted USB sticks are not available on Cardea or through the IT Department therefore the team / unit will need to purchase one from a reputable source for which the Trust will be reimbursed. The USB stick may need to be formatted prior to use therefore please check the manufacturer's instructions before use.

Before attempting to copy the footage, a request must be submitted via the Information Service Desk portal on the intranet for the USB stick to be unblocked. To ensure a prompt response, please provide the date that the footage will no longer be retained by the system with the other requested information.

The following steps should then be taken:

1. An unencrypted USB stick is plugged into the CCTV unit
2. The correct footage is identified and saved to the USB stick
3. A Trust computer is removed from the network
4. The USB stick is plugged into the computer and virus scanned
5. Once the virus scan is complete, the computer is reconnected to the Trust's network
6. A folder is created on a secure shared drive named with the date of the incident to enable easy location (restart may be required to access the drive)
7. The footage is saved to the secure folder
8. The footage is removed from the unencrypted USB stick

The Information Service Desk staff can provide assistance regarding removing and reconnecting a computer from the network and how to virus scan.

The USB stick must be stored in a secure location when not in use i.e. a locked desk drawer within a locked office and only be used for the specified purpose of transferring CCTV footage from the system to the shared drive.

It must never be used to transfer footage or other data around the Trust even within the same building as this presents a security risk.

## Appendix 6 - 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 | Information Department |
| Title | CCTV Procedure |
| Type | Procedure |
| Geographical area covered | Trust-wide |
| Aims and objectives | To give guidance to staff in all Trust locations where CCTV is in place 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**<br>• **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO**<br>• **Sex** (Men, women and gender neutral etc.) **NO**<br>• **Gender reassignment** (Transgender and gender identity) **NO**<br>• **Sexual Orientation** (Lesbian, Gay, Bisexual and Heterosexual etc.) **NO**<br>• **Age** (includes, young people, older people – people of all ages) **NO**<br>• **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO**<br>• **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and |

| | |
|---|---|
| | women on maternity leave) **NO**<br>• **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<br>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 |
| Describe any training needs for contractors or | N/A |

| | |
|---|---|
| other outside agencies | |

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

## Appendix 7 – 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? | N/A | Covered in CCTV Policy |
| | Are training needs included in the document? | N/A | Covered in CCTV Policy |
| **7.** | **Implementation and monitoring** | | |

| | Title of document being reviewed: | Yes / No / Not applicable | Comments |
|---|---|---|---|
| | Does the document identify how it will be implemented and monitored? | N/A | Covered in CCTV Policy |
| **8.** | **Equality analysis** | | |
| | Has an equality analysis been completed for the document? | Yes | |
| | Have Equality and Diversity reviewed and approved the equality analysis? | Yes | |
| **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 | |