# CCTV POLICY

# THE USE OF CLOSED CIRCUIT TELEVISION (CCTV) TO COMPLY WITH THE DATA PROTECTION ACT 1998

**Date of Issue: February 2015**

**Approved by: Health & Safety Committee**

**Review Date: February 2018**

**SAW/AM/CR**

# CCTV POLICY

***This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions***

| | | | |
|---|---|---|---|
| **Date of Issue:** | February 2015 | **Next Review Date:** | February 2018 |
| **Version:** | 4 | **Last Review Date:** | February 2015 |
| **Author:** | Steve Willicott Trust Security Manager/ LSMS<br>Alan McLaughlin Trust Security Manager/ LSMS<br>Charles Robinson Technical Security Officer/LSMS | | |
| **Director(s) Responsible** | Security Management Director<br>Director of Estates & Facilities Management | | |
| | | | |
| **Approval / Consultation Route** Health and Safety Committee | | | |
| **Approved By:** | | **Date Approved:** | |
| Trust Health and Safety Committee | | 28th February 2015 | |
| | | | |
| | | | |
| | | | |
| **Links or overlaps with other policies** | | | |
| Security Strategy | | | |
| Security Policy | | | |
| Trust Data Protection Policy | | | |

| Issue | Status | Date | Reason for Change | Authorised |
|---|---|---|---|---|
| V1 | Policy | July 2006 | Original Policy | Alan McLaughlin/ Charles Robinson |
| V2 | Policy | March 2011 | Review | Alan McLaughlin/ Charles Robinson |
| V3 | Policy | December 2013 | Addition of Appendix 2 CCTV on Patient Transport Vehicles | Alan McLaughlin/ Charles Robinson/ Peter Heath |
| V4 | Policy | | New Surveillance Camera Code of Practice 2013. Conducting privacy impact assessments | Alan McLaughlin/ Charles Robinson |

**CONTENTS**

## 1.0 INTRODUCTION

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act 1998 in respect of the use of CCTV (closed circuit television) surveillance systems managed by the Trust.

1.1 In drawing up this policy, due account has been taken of the following: -

- The Data Protection Act 1998; (DPA)
- Freedom of Information Act 2000 (FOIA)
- Surveillance Camera Code of Practice 2013 issued under the Protection of Freedoms Act 2012 (POFA code)
- The Human Rights Act 1998 (HRA)
- The Regulation of Investigatory Powers Act 2000
- Caldicott Report 1997.

1.2 The Data Protection Act 1998 came into force on the 1st March 2000 and contains broader definitions than those of its predecessor (1984) Act and more readily covers the processing of images of individuals caught by CCTV cameras. The changes in data protection legislation mean that for the first time legally enforceable standards will apply to the collection and processing of images relating to individuals.

1.3 An important new feature of the legislation is the Surveillance Camera Code of Practice 2013 which sets out the measures which must be adopted to comply with the Data Protection Act 1998. This goes on to set out guidance for the following of good data protection practice. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.

## 2.0 SCOPE

This policy will cover all employees of the Trust, persons providing a service (voluntary or paid) to the Trust, patients, visitors and all other persons whose CCTV image(s) may be captured by the system.

## 3.0 DEFINITIONS

3.1 Prior to considering compliance with the principles of the DPA, a user of CCTV or similar surveillance equipment, will need to determine two issues:

3.1.1 **The type of personal data being processed,** i.e. is there any personal data which falls within the definition of **sensitive personal data** as defined by Section 2 of the DPA;

'Sensitive personal data' includes:

- racial and ethnic origin;
- offences and alleged offences;
- criminal proceedings, outcomes and sentences;
- trade union membership;
- physical or mental health details;
- religious or similar beliefs;
- sexual life

3.1.2 The **purpose(s)** for which both personal and sensitive personal data is being processed. The data must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary
- processed in accordance with individual's rights;
- secure;
- not transferred to countries without adequate protection;

3.2 The Information Commissioner will take into account the extent to which users of CCTV and similar surveillance equipment have complied with this Code of Practice when determining whether they have met their legal obligations when exercising their powers of enforcement.

## 4.0 POLICY APPLICATION

### 4.1 Initial Assessment Procedures

4.1.1 The Chief Executive has the legal responsibility for the Trusts CCTV systems. However the Trusts Security Manager/ LSMS/ has responsibility for the day-to-day compliance with the requirements of the Surveillance Camera Code of Practice.

4.1.2 The purpose of the Trust's CCTV scheme is for:

- Detection and Prevention of Crime;

4.1.3 Prior to any camera installation the Security Manager/ LSMS will ensure that the installation complies with the Data Protection Act 1998 and Surveillance Camera Code of Practice.

4.1.4 **Privacy impact assessment:**

A privacy impact assessment looks at privacy in a wider context than just the DPA, it also takes into consideration the HRA (where the data controller is also a public authority), and the impact on privacy rights. It should look at the pressing need the surveillance system is supposed to address, and show whether or not the system will meet this need. It should be based on reliable evidence and show whether the surveillance system proposed can be justified as proportionate to the needs identified.

### 4.2 Siting the Cameras

4.2.1 It is essential that the location of the equipment be carefully considered, because the way in which images are captured will need to comply with the DPA.

4.2.2 All cameras are located in prominent positions within public and staff view and do not infringe on clinical / treatment areas. All CCTV surveillance is automatically recorded and any breach of these Codes of Practice will be detected via controlled access to the system and auditing of the system.

4.2.3 Signs have been erected on all entrance points to Trust premises and throughout the site to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signs must include details on the purpose, organisation and contact details.

4.2.4 Use of Covert CCTV (Directed) surveillance if required should be requested through the Police. If the request through the police is refused then authority can only be given by the NHS Security Management Service. This is covered by the Regulation of Investigatory Powers Act 2000 (RIPA).

## 4.3 Quality of the Images

4.3.1 It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme be 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.

4.3.2 All camera installations and service contracts should be undertaken by NACOSS approved security companies. Upon installation all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. All CCTV equipment should be serviced and maintained on an annual basis.

4.3.3 The system consists of cameras recording to digital recorders. These recorders are securely networked across Trust sites.

4.3.4 Viewing of live images on monitors should usually be restricted to the operator and any other authorised person where it is necessary for them to see it, for example to monitor congestion for health and safety purposes, unless the monitor displays a scene which is also in plain sight from the monitor location.

4.3.5 Where there is access to CCTV footage via the secure network, controls should be put into place so only authorised users are able to use it

## 4.4 Processing the images

4.4.1 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 and will be disposed of in a secure manner asap. 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.

4.4.2 All images are digitally recorded and stored securely within the systems hard drives, for up to 30 days when they are then automatically erased.

4.4.3 Where the images are required for evidential purposes in legal or Trust disciplinary proceedings, a cd-r disc recording is made and placed in a sealed envelope signed and dated and held by the Security Manager/ LSMS until completion of the investigation. Viewing of images within the security Office is controlled by the Security Manager/ LSMS or a person nominated to act on his behalf. Only persons trained in the use of the equipment and authorised by the Security Manager/ LSMS can access data.

4.4.4 Criteria for the viewing of images by non-security related personnel:

At the discretion of the responsible officer, individuals may be allowed to view images:

- If they are investigating an untoward incident
- In the case of a missing patient
- To identify persons relating to an incident

Areas which would normally result in permission being refused include:

- Where the person wishing to view has no connection with the incident or has no management role relating to an incident
- Where viewing is purely salacious
- Where the performance of a member of staff not relating to crime, fraud or the investigation of untoward incidents is involved.

Access to the recorded images must be restricted to a manager or designated member of staff. All accessing or viewing of recorded images must only occur within a restricted area and other employees should not be allowed to have access to that area or the images when a viewing is taking place.

If images are to be specifically retained for evidential purposes i.e. following an incident, break-in etc.; then these will be retained in the Trust Security Managers-LSMS office to which access is controlled.

Requests may be granted by the Trust Security Managers-LSMS and will arise in a number of ways, including:

- Requests for a review of images, in order to trace incidents that have been reported to the Police
- Immediate action relating to live incidents e.g. immediate pursuit
- Individual police officer seeking to review images.

Any request for recordings from the Police, in the process of their enquiries. Form (Appendix 1) must be completed and handed to the Trust Security Managers-LSMS before the Trust Security Managers-LSMS approves the release of the CCTV footage.

### 4.5 Access to and disclosure of images to third parties

4.5.1 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 continuity 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 Trusts' disciplinary procedure.

4.5.2 Access to the medium on which the images are displayed and recorded is restricted to Trust staff and third parties as detailed in the purpose of the scheme.

4.5.3 Access and disclosure to images is permitted only if it supports the purpose of the scheme. Under these conditions the CCTV images record book and the appropriate view / release form (Appendix 1) must be completed.

### 4.6 Access to images by individuals

4.6.1 Section 7 of the Data Protection Act 1998 gives any individual the right to request access to personal data. Individuals must make their request to access to the Trusts' Data Protection Lead who will determine whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties. If the duty of care cannot be discharged then the request can be refused.

4.6.2 A written response will be made to the individual, giving the decision (and if the request has been refused, giving reasons) within 40 days of receipt of the enquiry. If disclosure is appropriate a payment to the Trust may be required.

## 5.0 INTERACTION WITH OTHER TRUST POLICIES AND PROCEDURES

Data Protection Policy
Security Policy
Security Strategy

## 6.0 RESPONSIBILITIES

6.1 The Trusts Board has corporate responsibility for the implementation of this policy, monitoring its effectiveness and ensuring compliance with Surveillance Camera Code of Practice 2013 which is available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf or from the Trust's Security Manager/ LSMS.

6.2 The Trusts Board discharges this responsibility through the Director of Estates and facilities to whom the Trust Security Manager/ LSMS is accountable.

## 7.0 ENFORCEMENT

The Information Commissioner has the power to issue Enforcement Notices where it considers there has been a breach of one or more of the Data Protection Principles. An Enforcement Notice[i] would set out the remedial action that the Commissioner requires of the Trust to ensure future compliance with the requirements of the Act.

## 8.0 DOCUMENTATION

Copies of all documentation and records relating to the CCTV system will be held securely within Trust Security Managers-LSMS office and will be kept under restricted confidentiality, for a period of 6 years.

## 9.0 REVIEW

This policy will be reviewed every three years, or earlier in the light of changing circumstances by the Trust Security Committee.

**Appendix 1**

ACCESS TO VIEW OR COPY IMAGES-POLICE

| | |
|---|---|
| Name of person making Request: | |
| Organisation: | |
| Address: | |
| Telephone Number: | |

**DETAILS OF IMAGE TO BE VIEWED**

| | |
|---|---|
| Date: | |
| Reason: (For police only) | |

| | | | |
|---|---|---|---|
| Signed: | | Dated: | |
| Request Granted: | | Request Denied (Reason): | |

**TO BE COMPLETED IF IMAGES ARE REMOVED**

| | |
|---|---|
| **Ref. No.** | |
| **Issued To:** | |
| **Crime No: (for police only)** | |
| **Date Issued:** | |
| **Issued By:** | |
| **Return Date:** | |
| **I acknowledge receipt of the above CD:** | |

| | | | |
|---|---|---|---|
| **Signed:** | | **Date:** | |

**Appendix 2**

## CCTV on Patient Transport Vehicles.

The Transport Department is accountable to and will adhere to the South Devon Healthcare Trusts Close Circuit Television Policy.

**Variations to Sections within the above Policy**

**4.0 POLICY APPLICATION**

4.1.2 The purpose of CCTV on the vehicles will be for

a. Prevention or detection of crime or disorder.
b. Interest of public and employee Health and Safety.
c. Protection of Trust property and assets.

**4.2 Siting the cameras.**

4.2.3 Information signs will be erected on the side and rear door of the vehicle. (The purpose of the cameras is not to monitor patient activity)

4.2.4 Camera images will not be viewable within the vehicle. Data is stored on a memory card and accessed after the reporting of an accident or damage.

**4.4 Processing the images**.

4.4.2 Images are stored on an internal memory card for eight to sixteen hours and then automatically over written with new images.

4.4.3 Apart from the Trust Security Managers-LSMS only the Transport Manager and Operations Manager will be authorised to access/copy data from the memory card. This will be stored securely in a locked cupboard until required. The driver of the occurring incident will be notified of any images put into storage. A record will be kept of the date, time, and vehicle registration and by who took the card for storing.