NHS
West Suffolk
NHS Foundation Trust

Document ref. no: PP(22)250

CCTV Policy

For use in:	All areas of West Suffolk Hospital NHS Trust
For use by:	All Trust staff
For use for:	All Areas
Document owner:	Information Governance Manager
Status:	Approved

Contents

Summary/Preface

CCTV has become a common feature of our daily lives, supporting and aiding public confidence in its use is essential if its benefits are to be realised and its use is not to become increasingly viewed with suspicion as part of a surveillance society.

The West Suffolk Hospital NHS Foundation Trust believes that everyone has the right to their own privacy. In addition, we believe that there should be no interference by any public body with the exercise of this right except in accordance with the law, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

1. PURPOSE

The purpose of this policy is to ensure:

- That the use of Closed- Circuit Television (CCTV) adheres to the principles of the General Data Protection Regulations, Human Rights Act 1998,
- Regulation Investigatory Powers Acts 2000 and other relevant legislation.
- Meets the information Commissioner's office code of Practice
- That any CCTV system is not abused or misused.
- That CCTV is correctly and efficiently installed and operated.

2. SCOPE

The policy is binding on all employees of West Suffolk Hospital NHS Foundation Trust including Community Sites and applies also to other persons who may, from time to time, and for whatever purpose, be present on any of its premises.

3. POLICY STATEMENT

No CCTV scheme should be initiated, installed, moved or replaced without prior approval of the Information Governance Manager, the Caldicott Guardian must also be informed.

All schemes will be monitored and managed using the following procedures and must be formally approved (as above) prior to any installation.

1. Accredited Security Manager will assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment.
2. The assessment process and the reasons for the installation of the scheme will be clearly documented.
3. The purpose of the scheme will be documented in accordance with current legislation.
4. Assessment/findings will be shared with the Directorate involved.
5. The Accredited Security Manager is responsible on a day-to-day basis for the appropriateness of its use.
6. The Executive Director of HR and Communications will be informed of any CCTV footage that potentially identifies members of staff in any alleged criminal activity, gross misconduct or inappropriate behaviour.

4. PRINCIPLES

The following principles will govern the operation of all schemes:

1 All schemes will be operated fairly and lawfully and in accordance with the General Data Protection Regulations for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
2 All schemes will be operated with due regard for the privacy of all individuals at all times.
3 Any change to the purposes for which any scheme is operated will require the prior approval of the Information Governance Manager and/or the Accredited Security Management who inform the Chief Executive.

5. OWNERSHIP & OPERATION OF CCTV SCHEMES

All CCTV schemes are owned and operated by West Suffolk NHS Foundation Trust, including Community Sites. All cameras, monitors and data collection and retention processes are maintained operationally by the Accredited Security Manager, They will also monitor the use of all CCTV. The Information Governance Manager will provide advice and guidance on their use.

1 The Accredited Security Manager will assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment.
2 The assessment process and the reasons for the installation of the scheme will be clearly documented.
3 The purpose of the scheme will be documented in accordance with current legislation.
4 Assessment/findings will be shared with the Directorate involved.
5 The Accredited Security Manager is responsible on a day-to-day basis for the appropriateness of its use.
6 The Executive Director of HR and Communications will be informed of any CCTV footage that potentially identifies members of staff in any alleged criminal activity, gross misconduct or inappropriate behaviour.

7. KEY OBJECTIVES

1 To detect, prevent and reduce the incidence of crime on West Suffolk NHS Trust property; including Community Sites.
2 To reduce incidences of vandalism and criminal damage to the Trust, employees and visitors' property.
3 To ensure employee relations are open and transparent. Enhance the feeling of security provided to staff, service users and carers.
4 To enable the identification and subsequent apprehension and (prosecution) of offenders in relation to any crimes actually committed.
5 To assist the Trust in the enforcement of Disciplinary Policy and Disciplinary Rules.

8. RESPONSIBILITIES

It is the responsibility of West Suffolk NHS Trust as overall owner of all schemes:

1 To ensure compliance with this Policy;
2 To ensure that the operating procedures for all schemes are complied with at all times;
3 To ensure that the purposes and objectives of all schemes are not exceeded;
4 To notify all persons on the Trust property where CCTV is installed and that a CCTV scheme is in operation;
5 To facilitate formal subject access requests of any images captured under the terms of the General Data Protection Regulations.
6 To provide copies of this Policy when required to do so
7 The Executive Director of HR and Communications must be informed of any CCTV footage that potentially identifies members of staff in any alleged criminal activity, gross misconduct or inappropriate behaviour. In such cases, the individual staff member and if appropriate their union representative will have access to this CCTV footage.
8 In cases of potential fraud, the Director of Finance and the Trusts Counter Fraud Officer should be informed.

The Chief Executive is ultimately accountable for the manner in which the Trust utilizes CCTV.

Accredited Security Manager is responsible for ensuring that the sites within their locality which have CCTV are aware of this policy and implement its requirements.

Information Governance Manager is responsible for ensuring that systems and procedures are in place on the site for which they have responsibility to ensure compliance with this policy and the IC's Code of Practice and the General Data Protection Regulations.

9. DATA PROTECTION LEGISLATION

The hospital will identify and include all its CCTV use within the annual 'Notification' process required by the Information Commissioner.

All schemes will operate in accordance with the guidelines set out in the 'CCTV Code of Practice' and additional guidance published by the Information Commissioner.

10. TARGETED OBSERVATIONS

CCTV for targeted observation must be used only for specifically defined instances and in accordance with the declared purposes and objectives. The Regulation of Investigatory Powers Act 2000 regulates the use of covert/directed surveillance of this type and is subject to a strict code of practice. Use of CCTV in these instances or for any other reason other than that authorised in accordance with this policy is not permissible at any time or circumstance. Targeted Surveillance will only be permitted after legal advice has been taken, with approval of the Chief Executive for the Trust and the NHS Counter Fraud Authority to carry out this surveillance. The Information Governance Manger must be informed for Data Protection purposes.

11. INSTALLATION

The installation of all schemes must be in accordance with this policy and should remain appropriate to its original identified and documented business purpose in accordance with this policy.

12. CAMERA SIGNS

The Code of Practice requires that signs be placed so that the public are aware that they are entering an area which is covered by CCTV surveillance equipment.

The signs should contain the following information:

- identity of the person or organisation responsible for the scheme
- the purposes of the scheme
- details of who to contact regarding the scheme

13. MONITORING AND REVIEW

This policy, and the operation of West Suffolk NHS Trust's CCTV schemes will be reviewed regularly by the Trust's nominated Accredited Security Manager in consultation with the Information Governance Manager.

14. SUBJECT ACCESS

The Information Governance Manager or Accredited Security Manager, in response to a formal request from the data subject, will permit subject access to images monitored by the system either in hard copy format or by informal viewing. In instances where no recorded images are retained (instantaneous viewing only) data subjects will be informed that the system produces no recordable images and that subject access in these particular instances can only be granted for the purposes of determining the extent of the CCTV monitoring range only.

Release of information to the Police, Courts, or other legal bodies

From time to time, the police may request access to footage and/or copies on compact disc under the Police and Criminal Evidence Act. Such requests will only be made where: -

- A review of recordings is required to trace incidents which have already been reported to the police.
- Immediate action is required in relation to live/current incidents being pursued.
- A major incident has occurred.

In the case of civil disputes, access to footage or disks may be authorised through a Court Order.

Footage or disks may, in certain circumstances, be made available to lawyers acting for defendants, or victims, in connection with criminal proceedings.
The Health and Safety Executive is also empowered to seize footage or disks as part of an investigation they may be undertaking – if necessary without approval.

15. BREACHES OF THIS POLICY

The hospital will investigate any breaches of this policy, using appropriate mechanisms that may include disciplinary procedure.

As a major purpose of these schemes is in assisting to safeguard the health and safety of staff, service users and visitors, it should be noted that intentional or reckless interference with any part of any monitoring equipment, including cameras/monitor/back-up media, might be a criminal offence.

16. COMPLAINTS PROCEDURE

Grievances and complaints regarding the operation of the hospital's CCTV system may be progressed through the Trusts complaints process.

Author(s):	Sara Taylor, Information Governance Manager
Other contributors:	John Earnshaw, Security Manager
Approvals and endorsements:	
Consultation:	Trust Council. Unions
Issue no:	4
File name:	
Supercedes:	3
Equality Assessed	
Implementation	Policies will be checked by IG Manager. Published on Trust Website and distributed to all Managers for distribution to all staff. Published in the Greensheet
Monitoring: (give brief details how this will be done)	Monitoring will be spot checks that DPA compliance.
Other relevant policies/documents & references:	General Data Protection Regulations. Human Rights Act 1998 Regulation Investigatory Act 2000 Incident Policy Data Protection Policy Disciplinary Procedure PP (07) 040 CCTV Code of Practice: Information Commissioner (2008) CCTV Guidance and the General Data Protection Regulations - Good Practice Note
Additional Information:	

Appendix 1

OPERATIONAL PROCEDURES FOR THE CONTROL AND USE OF CCTV

In accordance with the CCTV Policy all installation and use of CCTV must be conducted in accordance with:

- The current CCTV Policy
- General Data Protection Regulations.
- Commissioners Code of Practice (CCTV) *(see information commissioner's office web site for latest issue*)
- The following operational procedures

Standards

Cameras

- Cameras must always be operated so that they will only capture the images relevant to the purpose for which the particular scheme has been established and approved.
- Cameras and recording equipment should be properly maintained in accordance with manufacturers guidance to ensure that clear images are recorded.
- Cameras should be protected from vandalism in order to ensure that they remain in good working order.
- If a camera/equipment is damaged or faulty there should be a separate local procedure for:

  >Defining the individual(s) responsible for ensuring the camera is fixed.
  >Ensuring the camera/equipment is fixed within a specific time period.
  >Monitoring and overseeing the quality of the maintenance work.

- Cameras should not be allowed/altered to view any areas outside of the boundaries of West Suffolk NHS Trust property without prior permission and involvement of the Information Governance Manager.

Operators

- All operators of CCTV equipment should be trained in their responsibilities in accordance with hospital policy and this procedure.
- All staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

Training

- 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.
- Training by camera installers will also be provided as appropriate.

Maintenance

- A comprehensive maintenance log will be kept which records all adjustments/alterations/servicing/non-availability of all individual schemes.
- If the system records location/time/date these will be periodically checked for accuracy and adjusted accordingly.
- Footage will not be retained for any longer than 31 days from the date of recording, and will be automatically overwritten
- A review must be undertaken at least annually to continually assess against the stated purpose of the identified scheme.
- Access to the recorded images should be restricted to a manager or designated member of staff.
- All accessing or viewing of recorded images should 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 the footage must be retained in a secure place to which access is controlled and a back-up made.

If footage is to be handed over to the Police or the NHS Fraud Counter Fraud Authority, a completed Schedule 2 Part 1 (2) of the Data Protection Act 2018 must be provided before any footage can be released.

Digital CCTV

- All digital CCTV systems installed on West Suffolk Hospital premises must have the storage capacity to hold a minimum of 21-day footage. In certain circumstances it may be considered appropriate to retain data for a longer period, a full risk assessment must be taken before deciding a longer retention period.

- Where digital CCTV is installed all sites must have local access to a DVD recorder that is compatible with the system in use.

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