Avon and Wiltshire Mental Health Partnership NHS Trust

Operation of CCTV Systems Policy

Board library reference	Document author	Assured by	Review cycle
P097	Paul Daniels	Quality and Standards Committee	3 Years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Introduction

Avon & Wiltshire Mental Health Partnership NHS Trust henceforth within this document referred to as the "Trust" is committed to providing a safe and secure environment for its staff, patients, carers and visitors and to maintaining the security of its premises and assets.

This policy will be applied to the fair treatment of all people, regardless of their gender, race, colour, ethnicity, ethnic or national origin, citizenship, religion, disability, mental health needs, age, domestic circumstances, social class, sexuality, beliefs, political allegiance or trades union membership. The Trust is firmly opposed to any discrimination based on these human characteristics and values.

2. Purpose or aim

It is the intention of this policy and associated policies to deliver a framework from which to operate Close Circuit Television (CCTV) systems to meet the Trust's legal responsibilities. The reason for this policy is to ensure that all CCTV is installed for the purpose ' To Detect and Prevent Crime' In particular, efforts will be focussed on ensuring: the protection of all staff, service users, carers and visitors, specifically minimising and preventing violence against those providing services; and the protection of Trust Property and assets, both financial and non-financial.

3. Scope

The policy covers all Trust property that has existing CCTV coverage and property being considered for CCTV coverage for the purposes of the safety and security of all staff, service users, Trust property and members of the public with a lawful reason to be on Trust property.

All cameras will be set only to view images that are intended for the objectives of the scheme and images recorded can only be used for the stated purpose of the system in the policy.

4. Policy Statement

The Trust believes that all staff, service users, carers and visitors should treat each other with dignity and respect and to behave in an acceptable and appropriate manner as set down in the Dignity at Work Policy. Staff have a right to work, as service users have a right to be treated, free from fear of assault and abuse in an environment that is properly safe and secure.

The Trust will ensure that systems are in place to provide a safe and secure environment for staff to work and provide the best clinical care for service users. Employees failing to observe this policy and applicable health and safety regulations may be subject to action in accordance with the AWP Disciplinary Policy and procedures.

By law any operator of CCTV is required to clearly state the objectives for using it and document the responsibilities of those involved in operating and managing the system.

The Data Protection Act 1998 was introduced to ensure that personal data is held accurately, securely, in a publicly accountable manner and is used only for intended and registered purposes. The Information Commissioners Office introduced the CCTV Code of Practice which has legally enforceable standards and points of good practice and this code imposes restrictions on the use of CCTV and other systems which capture images and the way in which evidence is gathered. Failure to abide with the proper procedures can leave a CCTV user exposed to civil and criminal liability.

5. Definitions

The term CCTV will apply to the use of close circuit television within the Trust to help support the reduction of the risk of crime in all forms within the organisation. It will apply to:

- **Crimes against individuals – violence and abuse**. (See Recognition Prevention and Management of Violence and Aggression Policy
- **Damage to and theft from premises.** (See AWP Standing Orders, Reservation and Delegation of Powers and Standing Financial Instructions)

6. Roles and responsibilities

6.1 Trust Board

The Trust Board is ultimately responsible for fulfilling legal requirements relating to all aspects of security including CCTV and it vests in the Chief Executive responsibility for the fulfilment of the relevant statutes

6.2 The Chief Executive

The Chief Executive takes specific responsibility for:

- Advising the Trust Board on the review of existing policy arrangements and allocation of resources to implement security related procedures.
- Referring matters of a critical nature to the Trust Board for resolution and ensuring that adequate security arrangements exist within the Trust.

6.3 Non-Executive Director

The requirement for a Non-Executive Director (NED) is set out in Secretary of State Directions to NHS Bodies on Security Management Measures 2004 (amended 2006). The role of the NED is to support, and where appropriate, challenge and support the Security Management Director on issues recommendations relating to security management at Executive Board level.

6.4 Executive Directors

On behalf of the Chief Executive the Director of Nursing and Quality takes lead responsibility for the management of Security within the Trust.

The Director of Nursing and Quality is also the nominated Security Management Director (SMD) and is the lead for Security at Board level. This is to ensure the monitoring of and compliance with Secretary of State Directions and subsequent guidance; and the requirements of NHS Protect in relation to measures taken to provide for effective Security Management.

The SMD will be responsible for ensuring:

- The promotion of safe working in all Trust operations.
- Overall professional responsibility for the accredited Local Security Management Specialist (LSMS) so that security management work is undertaken to the highest standard.
- The introduction, operation, monitoring and evaluation of this policy to ensure comprehensive, fair and consistent application throughout the Trust.
- In conjunction with the other Executive Directors, the provision of training, guidance and support to managers on the implementation of this policy.
- That employees are allocated clear responsibilities and receive adequate training in accordance with this policy.

6.5 Local Delivery Unit Directors, Clinical Directors and the Director of Facilities and Estates

All Directors are responsible for ensuring that for each service and department within their directorate:

- Complies with this policy and associated policies throughout their areas of responsibility and local arrangements that implement this policy are devised and reviewed.
- Will ensure that all relevant staff are conversant with the legal requirements when considering installing any CCTV. Guidance to follow when considering installing CCTV
  - Privacy Impact Assessment (PIA)
  - Data Protection Act 1998
  - Human Rights Act 2000
- Will ensure that all staff are conversant with legal requirements on all systems that are installed on Trust premises.
  - Signage
  - Processing Images
  - Evidence
  - Data Requests
  - Quality of Images
- Guidance for installed CCTV
- Within their area of responsibility, an owner of each system is identified with the responsibility for completing and updating an Areas of Coverage form, forwarding to their Support Service Business Manager and the LSMS. Required information for each system will include:
  - Site Name
  - Building Name
  - Camera Type, Fixed, Pan Tilt Zoom
  - Camera Location, where fixed to the building
  - Monitoring Station Location
  - System Operator
  - Maintenance Provider
  - Site Signage Yes/No
- That the identified owner completes the CCTV Annual Checklist (Appendix B) and returns it to the LSMS annually or when a system has been installed or modified.

6.6 Local Security Management Specialist (LSMS)

The Local Security Management Specialist will ensure that there is an owner identified for each system and that they are aware of their responsibilities under the Data Protection Act.

6.7 Information Governance Manager

The Information Governance Manager will ensure that the Trust has registered itself as a Data Controller with the Information Commissioners Office. The Data Protection Notification states the purposes for processing data, who are the data subjects and data classes. The Trust's Data Protection Officer, who is currently the Information Governance Manager, is responsible for ensuring that the Data Protection Notification is kept up to date. They will complete the Surveillance Camera Code of Practice Self-Assessment Tool to check compliance with the 12 guiding principles of the surveillance camera code of practice with assistance from the LSMS.

If there is any change in the stated purpose in this document form using CCTV, this must be formally communicated to the Data Protection Officer.

6.8 Line Managers

Each line manager has key responsibilities to ensure:

- Within their area of responsibility, that this policy is complied with and that employees are sufficiently aware of and conversant with this policy to perform their duties

6.9 Employees

All employees are to be conversant with this policy at a level sufficient to perform their duties (data protection).

7. Training

The Trust overarching policy for training is the Learning and Development Policy and this should be read in conjunction with this policy. Attached as appendices to that policy are the Trust's learning and development matrices. These matrices describe the minimum statutory, mandatory and required training for all staff groups in respect of Violence and aggression.

The Learning and Development Policy also describes the Trust's arrangements for training, in particular how there are processes in place to ensure staff receive the training they require and how non-attendance is followed up. These arrangements are further supported by management supervision and appraisal processes.

Basic training is provided on the Trust's Corporate Induction Day, and this should be followed by the relevant Information Governance training for the staff member's organisational job role. Training is provided centrally by Department of Health's "Connecting for Health". Additionally the Information Governance Team provides team and department training on request.

8. Risk Assessment

The Management of Health and Safety Regulations 1999 places a specific duty on employers to carry out risk assessments on the hazards that employees may be exposed to and determine what control measures need implementing to avoid or minimise the risks in so far as is reasonably practicable.

In compliance with statutory requirements and the directions of the Secretary of State to NHS bodies, risk assessments should be undertaken to ensure the:

- Physical security of the ward/department.
- Physical security of the assets and property in the ward/department.
- A risk assessment of physical security of premises and assets will be undertaken on an annual basis and also on change of use.
- Personal safety of staff, service users, carers and visitors in the ward/department and grounds.

Security risk assessments will be undertaken locally as indicated and required, e.g. following a change of use of the building, and as part of the regular risk assessment activity. The Trust's approach to risk assessment is described in the Risk Assessment Policy P054 and this includes a template for risk assessments in Appendix 4.

9. Standards

The Data Protection Act 1998 requires anyone who handles personal information to comply with a number of important principles. It also gives individuals rights over their personal information.

CCTV Code of Practice revised 2008 issued by the Information Commissioners Office taking into account of the technical, operational and legal aspects if CCTV.

10. Monitoring or audit

Implementation of this policy will be measured by a number of indicators including risk assessment activity via the Statutory Risk assessment schedule and team level returns from the annual health and safety assessment process. This enables the Trust to provide external bodies such as the NHS Litigation Authority, Health and Safety Executive and the Healthcare Commission with evidence and assurance of compliance with standards.

- Monitoring of team level returns from the annual health and safety self-assessment process. These monitor key aspects of the management of safety, building security, environment. Data from these is monitored by the Trust forums which set work plans based on key risks identified during the annual health and safety self-assessment process and a combination of external and internal security audits.
- The completion of the CCTV Annual Checklist by the identified owner will be returned to the LSMS. This information will be reported through the Health Safety Security and Fire Group.
- The completed Self-Assessment Tool will be reported through the Health Safety Security and Fire Group and saved on ourspace, this will be monitored and updated as required.

11. Archiving of Master Documents

This procedural document form part of a formal Trust record, and is to be managed in accordance with the Trust's records management policies and retention and disposal schedules.

An audit trail of all previous versions of this document is required for auditing purposes and will be automatically stored by the Board Library document repository.

The Board Library on Ourspace is the only recognised repository for master versions of procedural documents. Copies of this document must therefore not be stored elsewhere on the system, e.g. in workgroups. The library system will provide records management functionality to allow for the retrieval of previous versions of procedural documents stored on it.

12. References

Data Protection Act 1998

Freedom of Information Act 2000

Human Rights Act 2000

The Caldicott Principles

CCTV Code of Practice

Regulation of Investigatory Powers Act 2000 (as amended by the 2016 Bill)

13. Trust Policies, Procedures and Guidance Documents

Data Protection Policy P006

Risk Assessment Policy P054

Acceptable Use Policy P024

Information Security Policy P021

Overarching Information Governance Policy P020

Freedom of Information and Environmental Information Regulations Policy – P022

Disciplinary Policy and Procedure – P116

Bullying, Harassment, and Dignity at Work Policy P118

Areas of Coverage Form

Surveillance Camera Code of Practice Guide to the 12 Principals

Surveillance Camera Code of Practice Self-Assessment Tool

Guidance to follow when considering installing CCTV

Guidance for installed CCTV

14. Appendices

Appendix “A” – Access to View or Copy Images Pro forma

Click here to view document

Appendix “B”: CCTV Annual Checklist

Click here to view document

Appendix “C” CCTV Signage

Click here to view document

Appendix “D” – Information Leaflet CCTV

Click here to view document

Version History

Version	Date	Revision description	Editor	Status
1.0	02/11/2010	Approved by the Quality and Healthcare Governance Committee	DB/PAD	Approved
2.0	13/12/2011	Approved by the Quality and Healthcare Governance Committee	DB/PAD	Approved
2.1	20/01/2015	Planned review Inclusion of Self- Assessment Tool. Approved by Health & Safety Group	DB	Draft
3.0	17/02/2015	Approved by the Quality and Standards Committee	DB/PAD	Approved
3.01	16/01/2018	Draft for Health & Safety Group	DB	Draft
4.0	30/01/2018	Approved by the Health & Safety Group	DB	Approved