

MANCHESTER HEALTH ACADEMY

CCTV POLICY

CCTV POLICY

Approval History

Approved By:	Date of Approval	Version Approved	Comments
Governors	24/09/15	V2	

Revision History

Revision Date	Previous Revision Date	Rev	Summary of Changes	Changes Marked	Owner/Editor
11/09/2015		V2	Full Review	No	LMS

1. Purpose

The purpose of this policy is to manage and regulate the use of the CCTV system at Manchester Health Academy and ensure that:

- We comply with the Data Protection Act.
- The images that are captured are useable for the purposes we require them for.
- Reassure those persons whose images are being captured.

2. Scope

This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act 1998 and Information Commissioners Code of Practice 2008 and reference to “In the picture”: A data protection code of practice for surveillance cameras and personal information” from the Information Commissioners Office (October 2014) in respect of the use of CCTV (closed circuit television) surveillance systems managed by Manchester Health Academy.

3. Responsibility

Manchester Health Academy takes its responsibility towards the safety of staff and pupils very seriously. To that end, we use Closed Circuit Television (CCTV) cameras to monitor the members of our Academy in a very specific way.

This policy must be used in conjunction with the Academy Data Protection Policy.

4. Our Approach

Manchester Health Academy is fully committed to the safety of its staff, students and visitors and to this extent has invested in the security of its buildings and facilities.

5. Statement of Intent

The law states that we can use a CCTV system to monitor our premises, providing our system complies with the Data Protection Act.

The CCTV System includes static and sequential cameras and is used for the purpose of:

- The prevention, detection and investigation of criminal activity;
- The security of the premises;
- Safeguarding the safety of pupils, staff and visitors

This policy covers the use of CCTV and other systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Seeing what an individual is doing.

- Taking action relating to a crime.
- Using images of an individual in some way that could affect their privacy.

6. Objectives

The CCTV system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils and staff.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

7. Protocols

The CCTV system will be registered with the Information Commissioners' Office (ICO) under the terms of the Data Protection Act.

The system will comply with all additional legislation including:

- The Commissioner's Code of Practice for CCTV 2015.
- The Surveillance Camera Code of Practice 2013, published by the Home Office.
- The CCTV system is a closed digital system which does not make audio recordings and has no wireless capability.
- Warning signs have been placed throughout the premises where the CCTV system is active, as mandated by the Code of Practice of the Information Commissioner.
- The CCTV system has been designed for maximum effectiveness and efficiency. The Academy cannot however guarantee that every incident will be detected or covered and 'blind spots' may exist.
- The CCTV system will not be trained on individuals unless an immediate response to an incident is required.
- Additionally, the CCTV system will not be trained on private vehicles or property outside the perimeter of the school.
- Recordings will only be released following written authority from the Police, or in respect of a subject access request

8. Responsible Staff

The staff appointed to oversee the system and procedures are:

- The Facilities Managers Operationally
- Community Managers Viewing Only
- Senior Leadership Team Procedurally

9. Code of Practice

The CCTV is in operation 24/7 and is operated in accordance with the Surveillance Camera Code of Practice following guiding principles;

Manchester Health Academy has a CCTV surveillance system (the 'system') for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors.

The system is owned by the Academy and images from the system are strictly controlled and monitored by authorised personnel.

Its purpose is to ensure that the CCTV system is used to create a safer environment for staff, students and visitors to the Academy.

The system will:

- Always be for the purpose specified which is in pursuit of a legitimate aim.
- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point through which people can access information and complaints.
- Have clear responsibility and accountability for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the Academy.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access
- Consider all operational, technical and competency standards relevant to the system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access and use.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Be used only for the purposes for which it is intended, including supporting public safety, protection of pupils and staff and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

The CCTV is in operation 24/7 and is operated in accordance with the Surveillance Camera Code of Practice following the guiding principles below;

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need;
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified;

- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints;
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used. The images that are filmed are held in a secure location and can only be accessed by those who are authorised to do so;
- Clear rules, policies and procedures must be in place before surveillance camera system is used, and these must be communicated to all who need to comply with them;
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Every camera records simultaneously and the images are stored on the server for a period of 28 days. After that time, all images are erased apart from any which related to an incident subject to an ongoing investigation, which will be burnt onto a disc and saved onto the CCTV computer;
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes;
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards;
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use;
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published. Routine checks are made to ensure that the system is operating in accordance with the terms of this policy, and that information relating to the recordings (date, time etc.) are accurate;
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value; Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.
- The images that are filmed are held in a secure location and can only be accessed by those who are authorised to do so.
- Digital media is used to record images.
- The system has been set up to provide good quality images.
- Deleting of any stored data is only allowed with the principles permission.
- Routine checks are made to ensure that the system is operating in accordance with the terms of this policy, and that information relating to the recordings (date, time etc.) are accurate;

10. Security

Access to the CCTV system, software and data will be strictly limited to authorised operators and password protected.

Manchester Health Academy's authorised CCTV system operators are:

- | | |
|--------------------------|-------------------|
| • Facilities Managers | View and download |
| • Community Managers | Viewing Only |
| • Senior Leadership team | View and download |

The main control facility is kept secure and locked when not in use.

If covert surveillance is planned, or has taken place, copies of the authorisation forms and review will be completed and retained.

Camera systems will be maintained at all times.

Visual display monitors are located in the following offices.

- Facilities/Site Managers Office
- Sport shall Office

11. Privacy

Live and recorded materials will only be viewed by authorised operators for the purpose of investigating incidents.

Access by individuals

Requests for access will be handled in accordance with our Data Protection Policy.

All disks containing images belong to and remain the property of Manchester Health Academy.

Data handling procedures which are in place to ensure the integrity of the image information held can be found in our Data Protection Policy

Manchester Health Academy recognises the rights of staff, students and visitors to the Academy to make a subject access request for details of personal data held

Applications should be made in writing to the Principle or SLT

Access by the Police

Images, both still and moving, may be released to the police for the detection of crime under Section 29 of the Data Protection Act 1998

The request must be authorised by the Principal or a member of the SLT, specifying the date and time (as far as possible) of the image.

If the decision is taken not to release the images, then the image in question will be held and not destroyed until all legal avenues have been exhausted.

Viewing of images by the police will be recorded in a log.

Applications received from outside bodies (e.g. Solicitors) to view or release images will be referred to the Principal.

In circumstances where outside bodies make requests to view or release images, the Principal will normally release them provided satisfactory documentary evidence is produced to show that they are required for legal proceedings, a subject access request, or in response to a Court Order.

Images will only be retained for as long as they are required. The system will automatically delete recordings after 28 days.

Use of disclosure of images

Downloading images is strictly controlled and limited to the following staff:

- Facilities Managers. View and download
- Senior Leadership team View and download

All saved data must be handed to the Principal or a member of the SLT. Staff operating the system are trained to understand the administrative regime to control the use of the images.

12. CCTV – Use and Disclosure of Images Protocol

Legitimate public concerns exist over the use of CCTV and many of the specific guidelines are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is of fundamental importance that public confidence is maintained by fully respecting individual privacy.

Employees that are authorised to view the CCTV imaged within Manchester Health Academy must read this protocol alongside the CCTV Policy and confirm that they understand and agree to abide by the policy and protocol.

CCTV images may only be viewed by authorised employees named within this document.

All authorised employees viewing the CCTV images will act with utmost probity at all times.

All images viewed by authorised employees must be treated as confidential.

All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen.

Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the CCTV Policy.

All authorised employees viewing CCTV images should be aware of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. The viewers may be required to justify their interest in any particular individual, group of individuals or property at any time.

All authorised employees viewing CCTV images are responsible for their viewing of the images, which must be justifiable.

Any breach of the CCTV Policy or CCTV Protocol will be dealt with in accordance with existing discipline regulations. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

Any breach of the Data Protection Act 1998 will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this Act.

13. Related Documents

- Data Protection Policy
- Privacy Impact Assessment