The Sutton Academy

Use of CCTV Systems Policy

Status	**Non-Statutory**
Responsible Governors' Committee	**ALT**
Date first approved by GB	**Not Applicable**
Responsible Person	**Mr P Blakemore**
To Review Date	**March 2021**
Last Amended Date	**March 2019**

POLICY FOR THE USE OF CCTV SYSTEMS AT THE SUTTON ACADEMY

1. This Code of Practice is issued by The Sutton Academy Governing Body. It is intended to provide guidance as to good practice for users of the CCTV (closed circuit television) systems at The Sutton Academy.

2. This code is based upon the Code of Practice published by the Information Commissioner, which set out the standards that must be met if the requirements of the **General Data Protection Regulation** (**GDPR**) are to be met. These are that data should be:

    - *Fairly and lawfully processed;*
    - *Processed for limited purposes and not in any manner incompatible with those purposes;*
    - *Adequate, relevant and not excessive;*
    - *Accurate and where necessary kept up to date;*
    - *Not kept for longer than is necessary;*
    - *Processed in accordance with individuals' rights;*
    - *Secure;*
    - *Not transferred to countries without adequate protection.*

Objectives

The purposes of the CCTV Scheme in The Sutton Academy is to:

- Provide monitoring systems to assist with the protection of public property
- Assist in managing the academy
- Aid law enforcement, traffic management and community safety.
- Reduce crime and disorder.
- Improve the quality of life for the public in general.

Operators

1. The owner of the system is – Mrs A Sherman, Principal, The Sutton Academy, Elton head Road, St Helens, and Merseyside, WA9 5AU.

2. The general management of CCTV in The Sutton Academy is currently vested with the IT Network Manager, Mr Christopher Hopwood-Bell.

3. The day to day management of the CCTV system will also be the responsibility of Mr Christopher Hopwood-Bell.

4. Users of the CCTV system have the following profiles:
    a. The IT support team shall have full read, record and delete privilege.
    b. The leadership team, site management teams and the admin office personnel shall have read privileges.

5. CCTV viewing areas shall be the screens in the main office and IT support office.

Location of Cameras

1. The senior leadership have considered the proper location of CCTV cameras, where they exist, in and around The Sutton Academy.

   The location of the cameras is based upon a variety of information including security and health and safety. The positioning of CCTV outside washbasin areas of toilet blocks is to reduce vandalism.

2. All such CCTV equipment installed in The Sutton Academy will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.

3. If domestic areas such as gardens or areas not intended to be covered by the scheme border those spaces which are intended to be covered by the equipment, then the users should consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked. There are currently no cameras overlooking domestic areas

4. The employees and students will be made aware of the purpose(s) for which the scheme has been established and notices to this effect will be displayed in the academy reception area and the academy hall foyer.

5. The operators will only use the equipment in order to achieve the purpose(s) for which it has been installed.

6. Cameras that are adjustable by the operators will not be adjusted or manipulated by them to overlook spaces which are not intended to be covered by the scheme, other than as described in 7 below. There are currently no adjustable cameras.

7. If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators will be trained in recognising the privacy implications of such spaces being covered.

8. A sign, of no less than the minimum standard will be placed in the main entrance so that the public are aware that they are entering a zone that is covered by CCTV.

9. The signs shall be clearly visible and legible to members of the public.

10. The signs shall contain the following information:

    a. *Identity of the person or organisation responsible for the scheme;*
    b. *The purposes of the scheme;*
    c. *Details of whom to contact regarding the scheme;*
    d. *Any other information that may become a statutory requirement.*

Quality of Images

1. Upon installation an initial check will be undertaken to ensure that the equipment performs properly. Regular checks will be made thereafter to ensure that the system is operating properly.

2. Images are retained on a hard disc drive for a period of up to 30 days. Copies can be made for investigation purposes.

3. Checks will be made to ensure the accuracy of any features such as the location of the camera and/or date and time reference. Where the time/date etc are found to be out of sync with the current time/date, the operators will take such remedial action to correct the error.

4. Cameras will only be situated so that they will capture images relevant to the purpose for which the scheme has been established.

5. When installing cameras, consideration must be given to the physical conditions in which the cameras are located.

6. Cameras are to be properly maintained and serviced to ensure that clear images are recorded. Servicing will be carried out at least annually.

7. Cameras should be protected from vandalism in order to ensure that they remain in working order.

8. The IT Manager will:

    a. Be the person responsible for making arrangements for ensuring that a damaged camera is fixed
    b. Ensure that the camera is fixed within a specific time period.
    c. Monitor the quality of maintenance work and keep a record of any work done to the CCTV system.

Processing the Images

1. Images shall not be retained for longer than is necessary and unless required for specific investigation or evidential purposes, deleted after 31 days have passed.

2. Once the retention period has expired, the images shall be removed or erased. This currently happens automatically and where copies have been made on CD, said discs shall be shredded.

3. Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.

4. Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.

5. Access to recorded images shall be restricted to those staff outlined in the section on operators and any member of The Sutton Academy Staff who has been requested to attend the viewing for reasons of identification or assistance.

6. Viewing of the recorded images shall take place in a restricted area, for example, in a manager's or designated member of staff's office, other employees should not be allowed to have access to that area when a viewing is taking place.

7. Viewings and removal of the medium on which images are recorded, for viewing purposes, should be documented as follows: (Appendix A)

    a. The date and time;
    b. The name of the person;
    c. The name(s) of the person(s) viewing the images;
    d. The reason for the viewing;
    e. The outcome, if any, of the viewing;
    f. The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.

8. All operators and employees with access to images should be aware of the procedure that needs to be followed when accessing the recorded images.

9. All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of this policy and the rules on disclosure.

Access to and Disclosure of Images to Third Parties

1. All employees should be aware of the restrictions set out in this code or practice in relation to access to, and disclosure of, recorded images. A third party is anyone not designated with responsibility to view recorded images. Staff at The Sutton Academy without access rights to recorded images are to be considered third parties. The term recorded images does not include live images that are used in the main office since footage is live and users do not have access to recorded footage.

2. Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment. Staff who do not have access to the CCTV interface can request viewings and should seek the support of the academy technical team. Where a request to view video footage does not comply with the objectives of this policy the operator shall refuse the viewing.

3. All access to the medium on which the images are recorded should be documented by the operator regardless of whether this is done by the operator alone or with an additional member of staff. See Appendix A.

4. Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, disclosure will be limited to the following classes of persons/agencies.
    - Academy staff without CCTV access rights.
    - Law enforcement agencies, where the images recorded would assist in a specific enquiry.
    - Highways authorities in respect of traffic management matters.
    - Law enforcement agencies where the images would assist a specific criminal enquiry.
    - Prosecution Agencies.
    - Relevant legal representatives.

- All requests for access or for disclosure by third parties should be recorded, using the CCTV Log and where disclosure is denied a written response from the Principle shall be provided. The Principal shall have 40 days to respond to the request.

5. If access to or disclosure of the images is allowed, then the following will be documented. (Appendix A).
    - The date and time at which access was allowed or the date on which disclosure was made;
    - The identification of any third party who was allowed access or to whom disclosure was made;
    - The reason for allowing access or disclosure;
    - Location of the images
    - Any crime incident number to which images may be relevant
    - Signature of person authorised to collect the medium – where appropriate.

6. Recorded images will not be made more widely available – for example they shall not be routinely made available to the media or placed on the internet.

7. If for some reason it is intended that images will be made more widely available, that decision shall be made by the Principal or designated member of staff and the reason for that decision shall be documented.

8. If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

9. Operators should not delete any CCTV footage unless they have been instructed to do so, in writing by the Principal. A copy of the written order should be kept in the CCTV log file. If sensitive recorded footage is to be deleted it should be confirmed that any need for recorded footage for evidential reasons is no longer required before the footage is deleted.

Investigations requiring the use of CCTV

1. CCTV operators will not take any responsibility for investigating any incident requiring the use of CCTV other than to provide video evidence as it is required.

2. Where an incident is reported directly to the CCTV operator the responsibility for the investigation should be referred to the relevant member of staff which should be a member of Leadership, or Safeguarding teams. Where CCTV footage is identified that might assist with the investigation the operator should state as much to the investigator but should not produce copies of the video unless it is requested by the investigator.

3. Where images are being viewed in regard to an on-going investigation (either by the academy or law enforcement, highways agency etc.) it is essential that viewing does NOT take place in the presence/hearing of the data subject. If a data subject has for some reason seen the footage or printed photos through carelessness on the part of the operator or investigator, it should be reported to the police as this may affect the admissibility of it as evidence.

4. If an investigation is being conducted regarding a complaint or allegation against one of the designated CCTV operators, this should be reported directly to the Director of Operations so that access to the CCTV system can be denied immediately avoiding any chance for the staff member to tamper with or be accused of tampering with evidence. Where the complaint is about the IT Support Team, this should be reported directly to the Principal. The body investigating such a complaint should also be informed about steps taken to secure CCTV data.

Access by Data Subjects

1. In accordance with Section 7 of the Data Protection Act 1998 (Subject Access), an individual who believes that their image has been captured by this scheme is entitled to make a written request to the Principal. An investigation of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held.

2. All subject access requests should be referred in the first instance to the Principal.

3. All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and how such requests are to be dealt with.

4. CCTV Requests will be logged by the IT Support Team in the secure CCTV folder. The CCTV Log:
    - Indicates the information required in order to locate the images requested;
    - Indicates the information required in order to identify the person making the request.

5. Individuals, at the time of any subject access request, will be given a description of the type of images recorded and retained and the purpose for which the recording and retention takes place.

6. They should be informed of their rights as provided by the General Data Protection Regulation (GDPR).

7. Prior to any authorised disclosure, the Principal will need to determine whether the images of another “third party” individual features in the personal data being applied for and whether these third party images are held under a duty of confidence.

8. If third party images are not to be disclosed the Network Manager shall arrange for the third party images to be disguised or blurred.

9. If the Principal decides that a subject access request from an individual is not to be complied with a written reply shall be given.

Other Rights

1. Under the Data Protection Act individuals also have the following rights which may be applicable to CCTV schemes:
    a. Right to prevent processing likely to cause damage or distress.
    b. Rights in relation to automated decision taking.
    c. Right to seek compensation for failure to comply with certain requirements.

2. Where a request is made in relation to other rights, these shall be referred to the Principal who will document the request and respond to it.

Monitoring Compliance with This Code of Practice

1. The contact point indicated on the sign should be available to members of the public during normal office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.

2. Enquirers should be provided on request with one or more of the following:
    a. *A copy of this code of practice;*
    b. *The Complaints Procedure to be followed if they have concerns about the use of the system.*

3. The Director of Operations should undertake regular reviews of the documented procedures to ensure that the Code is being complied with.

4. An internal annual assessment should be undertaken which evaluates the effectiveness of the system.

5. De-personalised details of complaints will be maintained and will be included in an annual report on each CCTV system.

6. Complaints can be made in writing to the Principal. A copy of the academy complaints procedure can also be requested. Breaches and complaints shall be investigated by the Principal.

7. The IT Manager will review this policy annually and ensure the CCTV system is functioning correctly on a regular basis.

Appendix A

CCTV - Network Storage/Logging Policy

- CCTV recorded material is stored on the Staff Shared Drive (M Drive) in a secured access CCTV folder with a log file that needs to be recorded by the person dealing with the CCTV request.
- Viewing and recording of material is completed by the IT Support Team.
- The IT Team to view and record non sensitive incident requests
- The IT Manager to view and record sensitive incident requests
- Year Heads have access to view material folder relative the their Year Group
- ALT have access to view all year folders
- Saved files are to be moved to archive after 30 days, this folder is only accessible by ALT and IT Support.