Future Schools Trust

CCTV INFORMATION DOCUMENT

POLICY FOR THE USE OF C.C.T.V SYSTEMS AT FUTURE SCHOOLS TRUST

This Code of Practice is intended to provide guidance as to good practice for users of CCTV (closed circuit televisions) systems at Future Schools Trust. 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 Data Protection 1998 Act are to be met. These are listed below;

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*
- *Not kept for longer than necessary*
- *Processed in accordance with individuals rights*
- *Secure*

FUTURE SCHOOLS TRUST CCTV SYSTEMS

- Owner Operator Data and Controller of the Scheme – Tony Rice, Cornwallis Academy, Hubbards Lane, Maidstone, Kent, ME17 4HX.

- Future Schools Trust considers the CCTV scheme can contribute to the security and health and safety of all pupils, staff and visitors.

- The purpose of the CCTV scheme at Future Schools Trust is to provide monitoring systems to assist with the protection of the property, law enforcement, traffic management, community safety and the reduction of crime and disorder, thereby improving the quality of life for the public in general.

- CCTV systems at Future Schools Trust have been notified to the Information Commissioner.

- The general management of CCTV at Future Schools Trust is currently vested with the Facility Manager.

- The day to day management of the CCTV system is the responsibility of the Site Team.

SITING THE CAMERAS

The Governing Body Premises Committee has considered the proper location of the CCTV cameras, where they exist in and around Future Schools Trust Sites. The locations of the cameras are based upon a variety of information including security and health and safety.

Standards

- All CCTV equipment installed in Future Schools Trust will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.
- 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.
- The employees and pupils will be made aware of the purpose for which the scheme has been established and notices to this effect will be displayed in the school reception area. Parents will be informed through the school prospectus.
- The operators will only use the equipment in order to achieve the purpose for which it has been installed.
- 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 section A below.
- Signs, of no less than the minimum standard will be placed so that the public are aware that they are entering a zone that is covered by CCTV.
- The signs should be clearly visible and legible to members of the public.
- The size of the signs will vary according to circumstances.
- The signs should contain the following information.
    - *Identity of the person or organisation responsible for the scheme*
    - *The purpose of the scheme*
    - *Details of whom to contact regarding the scheme*
    - *Any other information that may become a statutory requirement*

(a) *If it is not physically possible 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.*

QUALITY OF IMAGES

Standards

- 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.
- Images are retained on a hard disc drive for a period of 31 days. Copies can be made for investigation purposes.
- 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 operator will take remedial action as is continued in the operations manual to correct the error. A note of such changes will be recorded in the occurrence log.
- Cameras will only be situated so that they will capture images relevant to the purpose for which the scheme has been established.
- When installing cameras, consideration must be given to the physical conditions in which the cameras are located.
- Cameras are to be properly maintained and services to ensure that clear images are recorded. Servicing will be carried out twice a year.
- Cameras should be protected from vandalism in order to ensure that they remain in working order.

PROCESSING THE IMAGES

Standards

- Images should not be retained for longer than necessary and unless required for specific investigation or evidential purposes, deleted after 31 days have passed.
- Once the retention period has expired, the images should be removed or erased.
- Images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.
- Access to the recorded images is restricted, and staff need to request access from a member of the **Senior Leadership Team** to decide whether to allow access.
- Viewing of the recorded images should take place in a restricted area. Other members of staff should not be allowed access to the area that viewing is taking place.
- Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows.
    - *The date and time of removal*
    - *The name of the person removing the images*
    - *The name of the person viewing the images*
    - *The reason for viewing*
    - *The date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.*
- All operators and employees with access to images should be aware of the procedure that needs to be followed when accessing the recorded images.
- All operators should be trained in their responsibilities under the Code of Practice.

ACCESS TO AND DISCLOSURE OF IMAGES TO THIRD PARTIES

Standards

All employees should be aware of the restrictions set out in the Code of Practice in relation to access to and disclosure of recorded images.

- Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose of using the equipment.
- All access to the medium on which the images are recorded should be documented.
- Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Subject to paragraph 1 above, in disclosure will be limited to the following classes or persons/agencies;
    - *Law enforcement agencies, where the images recorded would assist in a specific enquiry.*
    - *Law enforcement agencies where the images would assist a specific criminal enquiry.*
    - *Prosecution Agencies.*
    - *Relevant legal representatives*
- All requests for access or for discloser should be recorded, if access or disclosure is denied the reason should be documented.
- If access or discloser of the image is allowed, then the following will be documented
    - 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.
- Recorded images will not be made more widely available – for example they should not be routinely made available to the media or placed on the internet.
- If it is intended that images will be made more widely available, that decision should be made by the Director of Business Resources or designated member of staff and the reason for that decision should be documented.
- 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

ACCESS BY DATA SUBJECTS

Standards

- In accordance with section 7 of the Data Protection Act 1998 (subject access), and individual who believes that their image has been captured by this scheme is entitled to make a written request to the Academy Office. Upon payment of the current fee and the supply 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.
- All subject access requests should be referred in the first instance to the Director of HR or Head of Academy who will liaise with the Site Team.
- 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.
- Data subjects should be provided with a standard subject assess request form.
- 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. They should be informed of their rights as provided by the 1998 Act.
- Prior to any authorised discloser, we 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.
- If third party images are not to be disclosed the System Manager shall arrange for the third party images to be disguised or blurred.
- If the Director of HR or Head of Academy will decides that a subject access request from an individual is not to be complied with, the following should be documented.
    - *The identity of the individual making the request*
    - *The date if the request*
    - *The reason for refusing to supply the images requested*
    - *The name and signature of the person making the decision*

OTHER RIGHTS

Under the Data Protection Act 1998 individuals also have the following rights which may be applicable to CCTV schemes

- *Right to prevent processing likely to cause damage or distress*
- Rights in relation to automated decision taking
- Right to seek compensation for failure to comply with certain requirements

When a request is made in relation to other rights, these shall be referred to the Director of HR or Head of Academy, who will document the request and respond to it,

MONITORING COMPLIANCE WITH THIS CODE OF PRACTICE

Standards

- The contact point indicated in 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 if this equipment.
- Enquiries should be provided on request with one or more of the following
    - *A copy of this code of practice.*
    - *Subject access requests form if required or requested.*
- The Director of HR or Head of Academy should undertake regular reviews of the documented procedures to ensure that the provisions of the Code are being complied with.
- An internal annual assessment should be undertaken which evaluates the effectiveness of the system.
- Details of complaints will be maintained and will be included in an annual report on each CCTV system.