Use of Closed Circuit Television (CCTV) Policy

Introduction
This policy provides the procedures that must be followed for the use of CCTV systems.

The purpose of this policy is to regulate the management, operation and use of the CCTV systems at the Academy sites managed by the Solent Academies Trust.
The CCTV systems are owned by the Trust and the systems comprise of a number of fixed and moveable cameras located in and around the academies premises.

All cameras are monitored by selected senior staff together with those directly involved in the security of the academy sites

This policy follows the required data protection guidelines set out by the General Data Protection Regulation (GDPR).

Objectives
- To protect the Trust's buildings and their assets
- To increase personal safety and reduce fear of crime
- To support the Police in a bid to deter and detect crime
- To assist in identifying, apprehending and disciplining or prosecuting offenders
- To protect members of the public and private property

Statement of Intent
The Trust will treat the system and all information, documents and recordings obtained and used as data, which are protected by the GDPR.

Cameras will be used to monitor activities within the academies and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the academies, together with its visitors.

Staff have been instructed to ensure that static cameras are not able to focus on private homes, gardens and other areas of private property. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act, 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recorded materials will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recorded materials will never be released to the media for purposes of entertainment.

The planning and design has endeavored to ensure that the CCTV will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the school CCTV

Operation of the CCTV Systems
The systems will be administered and managed by the Director of Business and Operations, in accordance with the principles and objectives of this policy.

During the school day, management will be the responsibility of the site team, ICT team and selected Senior Leadership Team members. Out of hours and at weekends, management will be the responsibility of the site team.

The CCTV systems will be operated 24 hours each day, every day of the year.

Operational Control

- The site team will check and confirm the efficiency of the CCTV equipment daily and in particular that the equipment is properly recording.
- Access to the CCTV facilities will be strictly limited to selected Senior Leadership Team members, the site team and the ICT team, together with those directly involved in the security of the academy sites
- Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.
- The Senior Leadership Team must satisfy themselves regarding the identity of any visitors and the purpose of their visit. Where any doubt exists, access will be refused OR the CCTV images must be turned off.
- The systems may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual observations will not be permitted.
- If a maintenance emergency arises out of hours, Operational Controllers/Authorised Staff must satisfy themselves as to the identity and purpose of any contractor before allowing entry.
- Other operational functions will include maintaining recorded materials and hard disc space, filing and maintaining occurrence and system maintenance logs.

Liaison
Liaison meetings may be held as required with all staff involved in the support of the systems

Monitoring Procedures
Camera surveillance may be maintained at all times, pictures will be continuously recorded and No covert monitoring will be undertaken using the trust CCTV systems.

Recorded Material Procedures
In order to maintain and preserve the integrity of the recorded material used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each item of recorded material must be identified by a unique mark.
- Before use each item on which images will be recorded must be cleaned of any previous recording
- The person making the recording shall register the date and time of recorded material insert, including recorded material reference.
- Any recorded material required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure recorded material store. If recorded material is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence material store.
- If the recorded material is archived the reference must be noted.

Recorded materials may be viewed by the Police for the prevention and detection of crime, authorised officers of the Police for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of recorded materials to the Police or other authorised applicants. A register will be made available for this purpose.

Viewing of recorded materials by the Police must be recorded in writing and in a log book. Requests by the Police can only be actioned in accordance with current legislation.
Should recorded material be required as evidence, a copy may be released to the Police under the

procedures described Recorded Material Procedures part of this policy.

Recorded materials will only be released to the Police on the clear understanding that the recorded material remains the property of the trust, and both the recorded material and information contained on it are to be treated in accordance with this document.

The Trust retains the right to refuse permission for the Police to pass to any other person the recorded material or any part of the information contained thereon. On occasions when a Court requires the release of an original recorded material this will be produced from the secure recorded material store, complete in its sealed bag.

If the Police require the Trust to retain the stored recorded materials for use as evidence in the future, such recorded materials will be properly indexed and properly and securely stored until they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release recorded materials will be referred to the Director of Business and Operations. In these circumstances, recorded materials will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order.

Record Keeping/Incident Logs
The trust will maintain adequate and comprehensive records relating to the management of the system and incidents. Model documents from the installers/providers of CCTV system may be utilised for this purpose.

Retention of Data
There are no specific guidelines about the length of time data images should be retained. Consequently, the period of retention has been determined locally as 14 days. This is considered adequate unless determined otherwise.

- Where CCTV data is required to assist in the prosecution of a criminal offence, data will need to be retained until collected by the Police.
- Measures to permanently delete data should be clearly understood by persons that operate the system. These may be achieved by means of regular rotation of video tape(s) to ensure old data is overwritten or adjusting the image quality on disc based systems to ensure data is overwritten after a set period.
- Systematic checks should be carried out to ensure the deletion regime is strictly followed.

Breaches of the Policy (including breaches of security)
Any breach of the Policy by trust staff will be initially investigated by the Director of Business and Operations to determine disciplinary action, if necessary, and to make recommendations on how to remedy the breach.

Assessment of the CCTV System
Random checks will be undertaken on the CCTV system by the site team and ICT team, to evaluate its effectiveness.

Access by the Data Subject
Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

If the individual is not the focus of the footage i.e. they have not been singled out or had their movements tracked, then the images are not classed as ‘personal data’ and the individual is not entitled to the image under the provisions of Subject Access Request.

Requests for access should be submitted to:

The Data Protection Officer
Solent Academies Trust
c/o: Mary Rose Academy
Gisors Road
Portsmouth
PO4 8GT