Thomas Deacon Education Trust

Policy:	CCTV Policy
Owner:	Trust IT Lead
Approving Board:	Executive Group
Date of last review:	April 2025
Date of next review:	April 2027
Publish Status:	TDET website / SharePoint
Relevant to:	All TDET
Version:	2.0

Contents

1 CCTV Policy

The Trust recognises that CCTV systems can be privacy intrusive.

2 Objectives

Review of this policy shall be repeated regularly and whenever new equipment is introduced, a review will be conducted, and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the Trust in reaching the following objectives:

- To protect pupils, staff and visitors against harm to their person and/or property
- To increase a sense of personal safety and reduce the fear of crime
- To protect the Trust buildings and assets
- To support the police in preventing and detecting crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence; and
- To assist in managing the Trust.

3 Description of system

Cameras are based in internal and external locations within the Trust sites and may be fixed or movable.

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the Trust.

The CCTV system used by the Trust comprises of digital cameras sending images to NVR storage devices.

4 Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are prominently displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

The CCTV system will seek to comply with the requirements of both the Data Protection Act and the most recent Commissioner's Code of Practice.

The Trust will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured because of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the system 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, will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, considering the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 14 days.

Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), saved data will be retained for no longer than 6 months.

5 System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system for each site will be administered and managed by the designated member of staff for that site, who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the designated system manager, the system will be managed by the Trust Management & leadership teams.

The system and the data collected will only be available to the System Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Principal or Director of Resources.

The CCTV system is designed to be in operation 24 hours a day, 365 days a year though the Trust does not guarantee that it will be working during these hours.

The Site System Manager for each site will check and confirm the efficiency of the system regularly and that the equipment is properly recording and that the cameras

are functional.

Cameras have been selected and positioned to best achieve the objectives set out in this policy by providing clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such a request. Where any doubt exists, access will be refused.

Details of all visits and visitors to access CCTV footage, will be recorded in a site system logbook including time/date of access and details of images viewed and the purpose for so doing. Any internal requests for access to CCTV footage must go through the CCTV Access request form which can be found on the Trust's GDPR page. Requests from outside the school must go through the usual GDPR access request process.

6 Downloading Captured Data on to Other Media

To maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- Each downloaded media must be identified by a unique mark.
- Before use, each downloaded media must be cleaned of any previous recording.
- The System Manager will register in the access log the date and time of footage downloaded to external media, including its reference.
- Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a secure storage such as a safe or locked cupboard. If a downloaded media is not copied for the police before it is sealed, a copy may be made later providing that it is then resealed, witnessed and signed by the System Manager for the site, then dated and returned to the evidence store.
- If downloaded media is archived, the reference must be noted.
- If downloaded media is put onto a device, the device will be encrypted, and password protected.

Images may be viewed by the police for the prevention and detection of crime and by the site System Manager, his/her replacement and the Principal and other authorised senior leaders. However, where one of these people may be later called

as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence:

- For internal investigations footage may be viewed/extracted for evidence in situations that need justification for appropriate sanctions eg exclusions.
- For criminal investigations a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the Trust and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure storage, complete in its sealed bag.
- The police may require the Trust to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.
- Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to the Trust's Data Protection Officer and a decision made by a senior leader of the Trust in consultation with the Trust's Data Protection Officer.

7 Requests for Access by the Data Subject

The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Trust GDPR lead.

When a request is made, a member of the Academy or Trust management will review the CCTV footage in respect of the relevant time periods in accordance with the request.

If the footage only contains the individual making the request, the individual may be permitted to view the footage. This must be strictly limited to that footage containing the images of that individual.

If the footage contains other individuals the Trust must consider whether

- The request requires the disclosure of the images of any individuals other

than the requester, for example whether the images can be distorted so as not to identify other individuals.

- The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
- If not, then whether it is reasonable, in the circumstances, to disclose those images to the individual making the request.

8 Disclosure of images to Third Parties

The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images, then the member of the Academy or Trust Management must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for and any particular individuals of concern. This will enable proper consideration to be given to what should be disclosed and the potential disclosure of any third-party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure to CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to a disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

9 Public Information

Copies of this policy will be available to the public from the Trust office or on the Trust website.

10 Privacy Impact Assessment

Prior to the installation of any CCTV camera, or system, a privacy impact assessment will be conducted by the Trust to ensure that the proposed installation is compliant with legislation and ICO guidance.

11 Accountability

The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems located in restricted access areas
- CCTV system encrypted/password protected
- Ability to make copies restricted to specific members of staff

A record of access to CCTV images, including name of individual, time and date of access will be maintained by the Trust or staff member responsible at each site. This record will be made up of data acquired from the CCTV Access request forms.

The record must be kept, and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by the Academy or Trust Management in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- The individuals that were permitted to view the images and when; and
- Whether a copy of the images was provided, and if so to who, when and in what format.

12 Misuse of CCTV systems

The misuse of CCTV systems could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

13 Complaints relating to this policy or the use of CCTV

Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with the TDET Complaints Policy.

14 Monitoring, evaluation and review

This policy will be reviewed every 2 years or whenever a significant change to CCTV systems is made.