Thinking Schools Academy Trust

"Transforming Life Chances"

CCTV Policy

This policy was adopted on	November 2023
The policy is to be reviewed on	November 2027

1 Policy Statement

1.1 The Thinking Schools Academy Trust uses Close Circuit Television ("CCTV") within the premises of its Academies the purpose of this policy is to set out the position of the Thinking Schools Academy Trust as to the management, operation and use of CCTV.

1.2. This Policy applies to all Academies of The Thinking Schools Academy Trust and all Nurseries and Pre Schools of Little Thinkers Nursery & Pre School, a subsidiary of The Thinking Schools Academy Trust. When 'Academy' is used within this policy it applies to Nursery and Pre School settings. When 'Headteacher/Principal' is used with this policy it applies to Nursery Managers. When 'The Thinking Schools Academy Trust' is used within this policy is applies to Little Thinkers Nursery and Pre School.

1.3 This policy takes account of all applicable legislation and guidance, including:

1.3.1 General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 (together the Data Protection Legislation)

1.3.2 CCTV Code of Practice produced by the Information Commissioner

1.3.3 Human Rights Act 1998

1.4 This policy sets out the position of the Trust and its Academies in relation to its use of CCTV.

2 Purpose of CCTV

2.1 The Thinking Schools Academy Trust uses CCTV for the following purposes:

2.1.1 To provide a safe and secure environment for pupils, staff and visitors;

2.1.2 To assist with behaviour management and to ensure pupils take responsibility for their behaviour;

2.1.3 To prevent the loss of or damage to the Trust buildings and/or assets; and

2.1.4 To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders

3 Description of system

3.1 Cameras are based in internal and external locations within the Trust sites, different Trust sites will use analogue or digital cameras that may be fixed or movable. In some locations CCTV cameras may also record sound.

4 Siting of Cameras

4.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.

4.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. The Trust will make all reasonable efforts to ensure that areas outside of the Trust premises are not recorded.

4.3 Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

4.4 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

4.5 Some Trust/Academy sites utilise body worn CCTV cameras. Where body worn cameras are worn, persons wearing cameras are not permitted to enter areas where individuals have a heightened expectation of privacy.

5 Privacy Impact Assessment

5.1 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.

5.2 The Trust will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

6.1 The CCTV system will be managed by the Thinking Schools Academy Trust, Head of IT and Operations.

6.2 On a day to day basis the CCTV system will be operated by members of the Academy or Trust site management teams.

6.3 The viewing of live CCTV images will be restricted to Site Management Teams, Academy and Trust Management & leadership teams and other authorised persons who have been delegated permission by either the Trust's Executive Team or Academy leadership teams.

6.4 Authorised persons may include third parties who have a contractual arrangement with the Academy or Trust.

6.5 A list of authorised persons will be shared with each Academy's leadership team on an annual basis for review.

6.4 Recorded images which are stored by the CCTV system will be restricted to access by authorised persons as per 6.3. In the case of an incident being recorded on the CCTV images the Trust may share images with limited individuals who it deems are key in the management if the incident.

6.5 In addition, in some circumstances where it is necessary and proportionate to do so, the images may be shown to pupils involved in an incident either for the purpose of allowing that pupil to understand the impact of their behaviour or as part of the disciplinary process.

6.6 No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

6.7 The CCTV system is checked on a regular basis by Academy or Trust Site management and IT teams to ensure that it is operating effectively.

7 Storage and Retention of Images

7.1 Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

7.2 Recorded images are stored only for a maximum period of 28 days unless there is a specific purpose for which they are retained for a longer period. In such circumstances authorisation for holding recorded images longer than 28 days must be sought form the Head Teacher.

7.3 Legacy CCTV systems may not be capable of retaining recorded images for 28 days, depending on the resources available within the system.

7.4 The CCTV system should follow the principle of least privilege, with CCTV operators not having the ability to delete recorded images within the system. Any authorised persons who have permission to delete recorded images from the CCTV system must read and sign the Trust's Systems Administration Policy.

7.5 The deletion of recorded images within the CCTV system would be considered a breach of the Systems Administration Policy and may lead to disciplinary action as per the Code of Conduct.

7.6 Recorded images are stored locally within each CCTV system and are not backed up as part of the Trust's Business Continuity Plan.

7.7 In the event of a hardware fault that results in a loss of recorded images an incident report should be sent to the Head of IT and Operations and shared with the Head of

HR. The incident report should include a description of the fault, a timestamp when the incident was identified and the timeframe of images that has been lost.

7.8 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:

7.8.1 CCTV recording systems being located in restricted access areas;

7.8.2 The CCTV system being encrypted/password protected;

7.8.3 Restriction of the ability to make copies to specified members of staff

7.8.4 A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Trust

7.9 Appendix A provides an overview of existing CCTV systems across the Trust and indicates which system(s) meet the 28 day retention period and audit logging.

8 Disclosure of Images to Data Subjects

8.1 Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation, and has a right to request access to those images.

8.2 Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust's Subject Access Request Policy.

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

8.4 If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual member of the Academy or Trust management or leadership team must take appropriate measures to ensure that the footage is restricted in this way.

8.5 If the footage contains images of other individuals, then the Trust must consider whether:

8.5.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

8.5.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

8.5.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

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

8.6.1 When the request was made;

8.6.2 The process followed by the Academy or Trust Management or Leadership team in determining whether the images contained third parties;

8.6.3 The considerations as to whether to allow access to those images;

8.6.4 The individuals that were permitted to view the images and when; and

8.6.5 Whether a copy of the images was provided, and if so to whom, when and in what format.

9 Disclosure of Images to Third Parties

9.1 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.

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

9.3 If a request is received from a law enforcement agency for disclosure of CCTV images, then the member of the Academy or Trust Management or leadership 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 then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third party images.

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

9.5 If an order is granted by a Court for disclosure of 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 disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

10.1 This policy will be reviewed every 4 years

10.2 The CCTV system and the privacy impact assessment relating to it will be reviewed BI-ANNUALLY.

11 Misuse of CCTV systems

11.1 The misuse of CCTV system could constitute a criminal offence.

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

12 Complaints relating to this policy

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