Creating Tomorrow Trust

CCTV Policy

Purpose

This policy defines the set out the position of the Creating Tomorrow Trust, as to the management, operation, and use of CCTV.

Complied by: ITBP	**Date:** Jun 25
Committee: Finance & Resources Committee	**Date agreed by Trustees:** Jul 25
Review Cycle: Every 2 years with a 6 monthly review	**Review Date:** Jan 26

Wellbeing in our Trust

The responsibility for managing CCTV can be challenging and so this document aims to set out procedures to be followed to minimize what can be difficult pro cess.

We can all be affected by poor physical and mental health at times during our lives and it is important the appropriate support is available in a timely manner.

Health and wellbeing are everyone's responsibility, and we encourage an open and honest culture whereby anyone can discuss any issues they may have.

The Trustees of Creating Tomorrow take the health and wellbeing of all employees seriously and are committed to supporting our staff. The Trustees ensure that support for staff is available through:

- Effective line management.
- Commitment to ensuring an appropriate and balanced workload
- Supportive and professional working environments.
- Employee support programs:

The Education Support Line 08000 562561 or website https://www.educationsupport.org.uk/

Data Protection

Any personal data processed in the delivery of this policy will be processed in accordance with the Trust Data Protection policy.

1. Introduction

1.1 Creating Tomorrow Trust (the Trust) uses closed circuit television (CCTV) within the premises of its Academies. The purpose of this policy is to set out the position of the Trust as to the management, operation, and use of CCTV.

1.2 The system comprises of a number of fixed and dome cameras, vehicle and mobile dashcams.

1.3 The system has partial sound recording capability.

1.4 The CCTV system is owned and operated by the Trust and the deployment of which is determined by the CEO.

1.5 The CCTV is monitored centrally by the CEO of the Trust, or any senior member of Trust leadership that has this delegated.

1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the Trust community.

1.7 The use of CCTV, and the associated images and any sound recordings, is covered by the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

1.8 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the Trust data controller in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

1.9 This policy applies to all members of our Workforce, visitors to the Trust sites and all other persons whose images may be captured by the CCTV system.

2. Purpose of CCTV

Creating Tomorrow Trust uses CCTV for the following purposes:

2.1 To provide a safe and secure environment for students, staff, and visitors

2.2 To assist with behaviour management and to ensure students take responsibility for their behaviour.

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

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

3. Statement of Intent

3.1 The Trust complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at https://ico.org.uk

3.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the Trust sites, including gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the Trust will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area. There should be appropriate signage on School vehicles where dash cameras or internal CCTV is in use (see section 8).

3.3 The planning and design has endeavoured to ensure that the Scheme 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.

3.4 Treat the system and all information processed on the CCTV system as data which is covered by the Data Protection Act and UK GDPR.

4. Siting the Cameras

4.1 Cameras will be sited so they only capture images and audio relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The Trust will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act, this includes forward facing dashcams.

4.2 The Trust will make every effort to position cameras so that their coverage is restricted to the Trust's sites, which may include outdoor areas.

4.3 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

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 to avoid recording and storing excessive amounts of personal data.

6. Covert Monitoring

6.1 The Trust may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct.

ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

6.2 In these circumstances authorisation must be obtained from a member of the senior management team.

6.3 Covert monitoring must cease following completion of an investigation.

6.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, e.g. toilets.

7. Use of Personal Dashcams on Trust sites

7.1 Schools to communicate with Parent/Carers awareness of footage recorded by personal dashcams on Trust sites e.g. dropping off students/collecting students. Whilst the Trust allows personal dashcams that are installed in private vehicles, footage that contains personal data e.g. images of students, is for personal use and must not be shared without authorisation from the Trust or school where the footage was recorded.

8. Use of Dashcams in School vehicles

8.1 A prominent notice is placed in each vehicle stating, "This vehicle is equipped with a video monitoring system. Your actions may be recorded."

8.2 Access to video recordings from any security camera shall be limited to school administrators and Senior leadership. However, law enforcement officials may be granted access to video recordings after giving prior notice to School leadership. Additionally, in the event of an ongoing emergency in order to protect the health, welfare, and safety of all students, staff and visitors, Law Enforcement shall have immediate access to live video feed of security cameras. Law Enforcement shall notify the school senior leadership as soon as practical of the scope of such access.

8.3 Whenever conflicting accounts of a safety or disciplinary incident occurs, or if a parent or guardian disputes or challenges a bus discipline report, and the parent's child was video recorded, trust leadership may decide to review the recording. Neither the parent nor guardian of the student that has been video recorded, nor the student will be allowed to view the video recording in accordance with this policy.

8.4 The school or contracted vehicle operator will be responsible for the security of all bus digital video equipment and for the inserting and removing of video data storage device. When a school senior leader requests to view a recording, the contracted bus operator will safeguard the video data files until a meeting can be arranged. Digital files retained as part of an individual student's disciplinary record shall be maintained in accordance with law and School Committee

policy governing the access, review, and release of student records. All digital hard drive files will be erased/destroyed after a period of up to 30 days unless they are part of an ongoing investigation or of educational significance to the district.

8.5 Staff (unless authorised by the headteacher) are not allowed to view, download, delete, or share any data from the CCTV footage unless they are the vehicle operator and has been trained on the equipment, and has been requested to do so by a member of the senior leadership team. The school will not share any footage unless it is for a law enforcement agency or local government agencies that require the footage for an investigation.

9. Storage and Retention of CCTV images

9.1 Recorded data will not be retained for longer than 30 days, as per the Trusts Retention policy. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

9.2 All retained data will be stored securely.

10. Access to CCTV images

10.1 Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available.

11. Subject Access Request (SAR)

11.1 Individuals have the right to request access to CCTV footage relating to themselves under the UK GDPR. The request will be classed as a Subject Access Request (SAR).

11.2 All requests should be made in writing to the Information Manager (informationmanager@creatingtomorrow.org.uk). Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified e.g. date, time, and location.

11.3 The Trust will respond to requests within one month of receiving the SAR, timescale will commence after formal identification of the data subject making the request.

11.4 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 IT Team, as the CCTV system administrators, must take appropriate measures to ensure that the footage is restricted in this way.

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

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

11.6 The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

12. Access to and Disclosure of Images to Third Parties

12.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police, prosecuting organisations, and service providers to the Trust where these would reasonably need access to the data (e.g. investigators).

12.2 Requests should be made in writing to the Informationmanager@creatingtomorrow.org.uk

12.3 The data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

13. 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.

14. Complaints

14.1 Complaints and enquiries about the operation of CCTV within the Trust should be directed to the CEO of the Trust in the first instance.

15. Further Information

Further information on CCTV and its use is available from the following:

- https://www.gov.uk/government/publications/update-to-surveillance-camera-code
- https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/about-this-guidance/
- https://www.legislation.gov.uk/ukpga/2000/23/contents
- https://www.gov.uk/data-protection
- https://ico.org.uk