



THE CONSORTIUM
ACADEMY TRUST

CCTV Policy

The Consortium Academy Trust (TCAT)
An Exempt Charity Limited by Guarantee
Company Number 07665828

Status:	Live
Policy Owner (position)	CEO / DPO
Statutory / Recommended	Recommended
Date Adopted	16 July 2018
Review Date	Annual
Advisory Committee	Trust Board
Linked Documents and Policies	Data Protection Policy Freedom of Information Guidance ICT Acceptable Use Policy and Records Management Policy

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and Responsibilities
4. Location of Cameras
5. Purpose and Justification
6. Protocols
7. Security and Retention
8. Access to Footage
9. Use of Swipe Cards and Time Recording
10. Additional Information

Statement of intent

The Consortium Academy Trust (“the Trust”) takes the responsibility towards the safety of staff, visitors and pupils very seriously. To that end, where appropriate surveillance cameras are used across our academies to monitor any instances of aggression or physical damage to our premises and people on our sites.

The purpose of this policy is to manage and regulate the use of the surveillance and Closed Circuit Television (CCTV) systems used by the Trust and ensure that:

- We comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA)
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

This includes information recorded using any of the Trust’s swipe cards and time recording facilities

This policy should be read in conjunction with the following related Trust policies:

- Data Protection Policy
- ICT Acceptable Use Policy
- Records Management Policy
- Freedom of Information Policy

1. Legal framework

1.1. This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The GDPR
- The DPA
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

1.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO 2017) 'Overview of the General Data Protection Regulation (GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

2. Definitions

2.1. For the purpose of this policy the following definitions shall have the following meanings:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage. For the purpose of this policy only video footage will be applicable.
- Covert **surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

2.2. The Trust does not condone the use of covert surveillance when monitoring each academy's staff, learners and/or other visitors. Covert surveillance will only be operable in extreme circumstances where authorised by the Trust's DPO (see section 3.2 below)

3. Roles and responsibilities

3.1 The Trust is responsible for:

- Dealing with freedom of information requests and Data Subject Access Requests (DSAR) in line with legislation.

- Ensuring that each academy handles and processes surveillance and CCTV footage in accordance with data protection legislation.
 - Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
 - Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
 - Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.
 - Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the Trust, their rights for the data to be destroyed and the measures implemented by the Trust to protect individuals' personal information.
- 3.1. The DPO for the Trust is Gilly Stafford (Company Secretary/Clerk to the Trust), who is based at the Trust's headquarters at Cottingham High School and whose email address is dpo@consortiumtrust.co.uk. The DPO has responsibility for overseeing the operation of this policy.

4. Location of Cameras

- 4.1. The Trust operates a CCTV surveillance system at all of its academies.
- 4.2. Penshurst Primary School and Wolfreton School and Sixth Form College operate a video entry system at the main gates.
- 4.3. None of the systems listed above record audio footage.

5. Purpose and justification

- 5.1. The Trust uses surveillance footage in order to:
- Maintain a safe environment at each academy
 - Ensure the welfare of learners, staff and visitors.
 - Prevent and deter criminal acts against persons and property.
 - Assist the police in identifying persons who have committed an offence.
- 5.2. The Trust has considered alternatives to using CCTV, such as additional regular inspections of its premises, but has concluded that such alternatives would be less effective and more costly. In particular, there are situations that require a rapid response if the risk to learners', staff and visitors' security and safety is to be minimised. CCTV is the best way for the Trust to achieve this.
- 5.3. The Trust reserves the right to use CCTV footage in connection with any disciplinary action or other proceedings.
- 5.4. Under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facility.
- 5.5. The system will not be used:
- To provide recorded footage for the internet
 - For any commercial or entertainment purpose
 - For any automated decision taking

6. Protocols

- 6.1. The Trust has registered that it operates a CCTV surveillance system with the ICO in line with data protection legislation.
- 6.2. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. A related Privacy Statement explaining the Trust's use of the system (as required by the GDPR) has been posted online by the Trust and this website address is stated on each sign.
- 6.3. Footage recorded using each academy's CCTV system is monitored and recorded centrally at the relevant academy.
- 6.4. The surveillance system has been designed for maximum effectiveness and efficiency.
- 6.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.
- 6.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of any academy.

7. Security and retention

- 7.1. Access to the surveillance system, software and data (including visual display monitors) is strictly limited to authorised operators as designated by the relevant academy and will be password protected. A log of access to CCTV footage will be maintained by each academy.
- 7.2. Nobody other than authorised Trust personnel are permitted access to footage generated by any of the Trust's CCTV systems without specific authorisation from the DPO. Any individual who accesses CCTV footage without such authorisation could also be committing a criminal offence.
- 7.3. The main control facility at each academy is kept secure and locked when not in use.
- 7.4. Each academy will have a separate system that can be run independently of one another.
- 7.5. Any cameras that present faults will be repaired as soon as is reasonably practicable as to avoid any risk of a data breach.
- 7.6. Footage will not be removed from the system itself other than in accordance with this policy. All footage recorded using the systems will be retained for up to 30 days from the date of the recording and then automatically overwritten. Any footage copied from the system for a purpose set out in this policy will be retained for a reasonable period (determined by the DPO) having regard to the reason for copying the footage.

8. Access to footage

- 8.1. All non – routine access to, and disclosures of, CCTV footage must be recorded in the relevant academy's CCTV log. Such records must include details of the accessor / recipient of the footage and the date and reason for the access / disclosure.
- 8.2. All requests for access to footage recorded using the Trust's CCTV systems (including but not limited to requests from law enforcement agencies and DSARs) must be

referred to the DPO. No such footage shall be disclosed to any third party or unauthorised employee without specific authorisation from the DPO. Any such disclosure should be proportionate having regard to the purpose of the footage being requested (e.g. if a law enforcement agency asks to see footage of an incident which occurred at a specific time, the amount of footage disclosed should be limited to footage from around that time).

- 8.3. In the event that any footage is provided to law enforcement agencies, this shall be by making it available for them to view at the relevant Trust premises unless otherwise authorised by the DPO.
- 8.4. Any DSAR for CCTV footage will be handled in accordance with the Trust's Data Protection Policy.

9. Use of swipe cards and time recording

- 9.1 We recognise the importance of recording accurately the times when you are at work to ensure that you are paid in accordance with your contractual rights. We also need to be able to ascertain at any time whether you are on our premises in the event of a fire or other emergency and that only authorised personnel have access to those sites which have greater security concerns. We have recognised that our CCTV systems are not suitable for these purposes.
- 9.2 Having considered a number of alternatives such as maintaining a manual register and using combination door locks, we have concluded that the most effective and efficient way to achieve our objectives is to put a number of electronic time recording and security mechanisms in place at various sites.
- 9.3 Employees working at certain sites are given an electronic swipe card which they must use to access the workplace. In doing so, we are able to verify instantly who is on our premises at any given time and for how long they have been there. Swipe cards also help to make the relevant areas on our sites secure from intruders.
- 9.4 If you are issued with a swipe card or other electronic monitoring device and lose it or suspect it has been stolen, please contact the DPO immediately so that it can be deactivated. If you do not do so, unauthorised persons may be able to gain access to our premises and we may not be able to properly monitor your working hours and whereabouts to ensure that you are paid in accordance with your contractual rights.
- 9.5 Although the primary reason for installing the time recording and security equipment is to restrict access to our premises and assist in the proper recording of your working hours and whereabouts for safety purposes, we reserve the right to use information learned from swipe card logs and other time and location recording equipment as evidence in misconduct and performance-related investigations, as well as in disciplinary and court proceedings.
- 9.6 Any stranger seen in entry-controlled areas should be reported.

10. Additional Information

- 10.1 This policy does not form part of any employee's contract of employment and it may be amended by the Trust at any time. Any changes will be notified to you in writing.

- 10.2 If you are found to be in breach of the terms of this policy you may be subject to disciplinary proceedings which in serious cases, or in cases of repeated breach, may result in dismissal (and, in exceptional circumstances, criminal charges). If you are in any doubt about the terms of this policy or have any questions or complaints in relation to the Trust's CCTV systems or the operation of this policy, please contact the DPO