chaseterraceacademy

Closed Circuit Television (CCTV) Procedure

Partner school

John Taylor Multi Academy Trust

Statement of intent
Chase Terrace Academy takes the responsibility towards the safety of students, staff and visitors very seriously. The school uses surveillance cameras to monitor any instances of aggression or physical damage to school property and its members. The purpose of this policy is to manage and regulate the use of the surveillance and closed-circuit television (CCTV) systems at the school and ensure that:

- we comply with data protection legislation, including the Data Protection Act 1998 and the General Data Protection Regulation (GDPR);
- the images that are captured are useable for the purposes for which we require them; and
- we reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This procedure covers the use of surveillance and CCTV systems that capture moving and still images of people who could be identified, as well as information relating to individuals. This is used in order to:

- observe what an individual is doing;
- take action to prevent a crime;

Using images of individuals could affect their privacy and it is important, therefore, that there is a clear and legitimate framework for this activity.

Legal framework
This procedure has due regard to legislation and statutory guidance, including, but not limited to the following:

- The Regulation of Investigatory Powers Act 2000;
- The Protection of Freedoms Act 2012;
- The General Data Protection Regulation (GDPR);
- The Data Protection Act 1998;
- 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.

This policy operates alongside the JTMAT Data Protection (GDPR) Policy and has been created with regard to the following statutory and non-statutory guidance:

- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'.

Linked policies
This procedure should be considered in conjunction with the following JTMAT policies:

- Data Protection (GDPR) Policy
- Records Management (GDPR) Policy
- Safeguarding Policy
- CCTV Policy (JTMAT)

Definitions
For the purpose of this procedure, a set of definitions are outlined, in accordance with the surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals, including video, audio or live footage. For the purpose of this procedure, only video and audio footage will be applicable;
- Overt surveillance – any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000;
- 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;
- Playback – viewing of recorded footage within the CCTV system;
- Exported footage – footage that has been downloaded from the CCTV system, making it viewable outside of the CCTV software, and in a format that can be shared as needed;
- NVR – Network Video Recorder; a hardware device attached to the school network, which manages a number of cameras, storing their recordings and facilitating access to footage.

Chase Terrace Academy does not condone the use of covert surveillance when monitoring the school's staff, students and/or volunteers. Covert surveillance will only be operable in extreme circumstances. Any overt surveillance footage will be clearly signposted around the school.

Purpose and justification

The school will only use surveillance cameras for the objectives stated in this procedure. Surveillance will be used as a deterrent for violent behaviour and damage to the school property. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and CCTV cameras be present in any toilet cubicle or changing facility. If the surveillance and CCTV systems fulfil their purpose, and are no longer required, the school will deactivate them.

Data collected from surveillance and CCTV will be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes - further processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up-to-date - every reasonable step will be taken to ensure that personal data that is inaccurate (having regard to the purposes for which it was processed) is erased or rectified without delay;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed - personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Objectives
The surveillance system will be used to:

- strengthen the security of the school site and property;
- monitoring the safety and safeguard students, staff and visitors;
- promote and enhance the safety of all occupants;
- aid internal investigations;
- prevent the destruction of property;
- recovery losses - as a result of destruction of property;
- enforcement the school's Behaviour Policy; and
- provide evidence to law enforcement agencies, as required.

Siting
When siting cameras, consultation will be carried out with the relevant personnel, at which point the intent for the camera will be established and recorded. Camera location will be considered against the requirements of the Data Protection Act and the ICO's CCTV Code of Practice.

A visual map of CCTV camera locations, and the areas covered by these is held internally, to be reviewed annually, and when assessing the location of new cameras.
The school will take any steps necessary to ensure that expectations of reasonable privacy are not violated by the location of a CCTV camera.

The school will ensure that, within reason, CCTV footage is restricted to school property only and will not encroach on the privacy of unrelated individuals or residences. Employees of the school have access to details of camera location, except in the exceptional circumstances where a camera has been located for the purpose of covert monitoring.

In some circumstances, it may be required to place camera equipment in areas that are deemed to be sensitive during the initial consultation. The Headteacher, Designated Safeguarding Lead (DSL) and the Trust Data Protection Lead will be consulted to ensure that reasonable privacy has not been violated. The DSL will be responsible for auditing the continued integrity of this installation (as part of the school's safeguarding audit process).

For the purpose of safeguarding students, maintaining good hygiene and preventing vandalism, CCTV is fitted in the washroom areas adjacent to student toilets. This is done in such a way that students' privacy is not compromised. Cameras are used to monitor the following areas:

- sinks
- doors in/out of the toilet block
- The cameras do not have any view of inside, or above, toilet cubicles or urinals

Physical and electronic security measures are in place to prevent tampering with any of the cameras.

Protocols
The surveillance system will be registered with the ICO in line with data protection legislation. The surveillance system is a closed digital system which does not record audio. Warning signs have been placed at all entrances to the premises, as mandated by the ICO's Code of Practice. The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist. The surveillance system will not be trained on individuals unless an immediate response to an incident is required. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

Security
A range of measures may be taken to ensure a consistent level of security across the site. These can include, but are not limited to, the following:

- limiting use to authorised operators and through the use of secure passwords;
- utilising different access levels;
- auditing access to CCTV systems;
- locating recording equipment in restricted and/or monitored areas;
- encrypting data on drives and during network transmission;
- physically obscuring and securing equipment such as recorders, cabling and power supplies from general access;
- including physical security measures to prevent tampering or adjustment (where camera equipment is placed in sensitive areas);
- completing audit checks - to ensure the integrity of the system

Privacy by design
The use of surveillance cameras and CCTV is critically analysed using a data protection impact assessment. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means. If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

Covert monitoring
In exceptional circumstances, there may be a requirement for the school to implement covert monitoring with CCTV recording equipment. Examples of these circumstances include:

- where there is good cause to suspect that an illegal or unauthorised action is taking place, or where there are grounds to suspect serious misconduct; and
- where notifying the individuals about the monitoring would seriously prejudice the reason for the monitoring.

Covert monitoring must be approved by the Headteacher, or in cases where this may prejudice the outcomes, the Chair of the Local Governing Body. Covert monitoring must cease on the completion of the relevant investigation.

Camera equipment installed for covert monitoring will not violate the expectation of reasonable privacy.

Code of practice
The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. The school notifies all students, staff and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All surveillance footage will be kept for 30 days for security purposes; the Headteacher is responsible for keeping the records secure and allowing access.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, students and visitors. The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, students and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

The surveillance and CCTV system will:

- be designed to take into account its effect on individuals and their privacy and personal data;
- be transparent and include a contact point, the DPO, through which people can access information and submit complaints;
- have clear responsibility and accountability procedures for images and information collected, held and used;
- have defined policies and procedures in place which are communicated throughout the school;
- only keep images and information for as long as required;
- restrict access to retained images and information with clear rules on who can gain access;
- consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law;
- be subject to stringent security measures to safeguard against unauthorised access;
- be regularly reviewed and audited to ensure that policies and standards are maintained;
- only be used for the purposes for which it is intended, including supporting public safety, the protection of students, staff and volunteers, and law enforcement;
- be accurate and well maintained to ensure information is up-to-date.

Storage and retention of recorded images

Footage is recorded digitally and stored within school on Network Video Recorders (NVRs). This footage is captured and stored on NVRs will be automatically overwritten at the end of the predetermined retention period, which is set and stored internally. Footage extracted from NVRs will not be stored for longer than necessary. Whilst 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.

This extracted footage will be stored in accordance with the Data Protection (GDPR) Policy and Records Management (GDPR) Policy.

Access to, and disclosure of, recorded Images

An internal register of individuals authorised to access the CCTV system is maintained within the school. The individuals that make up this list include:

- senior leadership;
- pastoral staff;
- safeguarding staff;
- ICT staff;
- Site staff.

The internal register is a record of individuals that have undergone training and had a risk assessment completed for, to ensure that authorisation is required for the school's CCTV system to meet its objectives without risk of compromising the integrity of the system. Only after these steps have been completed, will a person be granted individualised access to the CCTV system.

Authorised individuals are to use common sense to ensure that footage is witnessed by other persons, unless they are explicitly relevant in helping to resolve the issue being investigated without any conflict or risk of interrupting an investigation. Recorded or live footage may be viewed by authorised individuals without formal notification, providing it is for a valid purpose, as defined within this document.

A record is to be made any time footage is extracted from the CCTV system by an authorised individual. This record includes the time and date, name of the individual extracting footage and a summary outlining the purpose for extraction. This record will be subject to regular review by the Headteacher, to ensure compliance with all procedures as outlined in this policy document and to ensure that footage is securely erased once it is no longer required.

Extracted footage is to be stored in a single, secure location, only accessible to authorised CCTV users except in circumstances where footage is sensitive in nature. Under these circumstances, a secure network location only accessible to the Headteacher will be used initially; the Headteacher maintains the authority to delegate access to individuals as necessary. Any delegation will be recorded centrally.

Extracted footage is to strictly remain on school owned devices and only accessed over the secure school network. Footage is never to be copied on to removable media or cloud storage. Extracted footage is only to leave the school with authorisation from the Headteacher, or Deputy Headteacher in their absence.

A CCTV Request form is to be completed and signed by the authorising individual and the third party before footage is handed to the third party. One copy is to accompany the footage, and another to be kept on file in the school. A copy of the footage is to be retained in school for a period of at least 6 months, or until the matter relating to the footage has been resolved. Footage can only be transferred by the Headteacher, PA to Headteacher, Deputy Headteacher, Business Manager and in their absence, the Network Manager. The school's preferred media for transfer is a labelled CD-ROM. Requests for other media will be considered on a case-by-case basis, this will be recorded on the transfer form.

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Further information can be found in the Data Protection (GDPR) Policy. Requests for Data Subject Access should be made to the Headteacher. Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry;
- Prosecution agencies – such as the Crown Prosecution Service (CPS);
- Relevant legal representatives – such as lawyers and barristers;
- Persons who have been recorded and whose images have been retained, where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000.

Requests for access or disclosure will be recorded. The Headteacher will decide whether recorded images may be released to persons other than the police, consulting with the Trust's Data Protection Lead.

Reviewed by Governing Body: June 2023
Adopted: June 2023
Next Review: June 2025

Appendixes

CCTV Signage

CCTV Request Form

Requester Name		Date of Request	
Location of Incident to be Reviewed			
Time of Incident to Be Reviewed			
Reason for Request			
Approver Name		Approver Signature	
		Date / Time	

Address of requester if external	

To be completed by the Operator

Which Cameras Observed	
Copies Made? (Yes / No)	
Media (circle)	CD-ROM / Memory Stick / Cloud / Secure Email / Other _____
Police Crime Number if relevant	