CCTV Policy

This policy should be read in conjunction with the Trust's Data Protection (GDPR) Policy and Records Management (GDPR) Policy. These are available on the SSMAT website and from the CTA website.

POLICY APPROVAL and REVIEW

Review date: ***Sep. '20***

Approval needed by: ***Trust Board / Finance, Audit and Risk Committee***

Adopted: ***Sep. '20***

Next review date: ***Nov. '22***

Closed Circuit Television (CCTV) Policy

Statement of intent

At Chase Terrace Academy, we take our responsibility towards the safety of students, staff and visitors very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school 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 policy 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:

- observing 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 policy 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 SSMAT Data Protection (GDPR) Policy and has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'

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

Linked policies

This policy should be considered in conjunction with the following SSMAT policies:

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

Definitions

For the purpose of this policy, 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 policy, 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.

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.

Roles and responsibilities

DATA PROTECTION OFFICER

The role of the Data Protection Officer (DPO) is played by the Trust Business Manager and includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process 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 consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the GDPR.
- 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 school; their rights for the data to be destroyed; and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.

- Reporting to the Trust Board (Finance, Audit and Risk Committee).
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's Data Protection Impact Assessment (DPIA), and providing advice where requested.

DATA CONTROLLER

The role of the Data Controller is played by the Executive Headteacher, on behalf on the Trust Board. The Data Controller determines the purposes and means of processing personal data.

DATA PROTECTION LEAD

The role of the Data Protection Lead is played by the Academy Business Manager deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the Data Controller. The role of the Data Controller includes:

- processing surveillance and CCTV footage legally and fairly;
- collecting surveillance and CCTV footage for legitimate reasons, ensuring that it is used accordingly;
- collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection;
- ensuring that any surveillance and CCTV footage identifying an individual is not kept for any longer than is necessary; and
- protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure, especially when processing over networks.

HEAD OF SCHOOL

The role of the Head of School includes:

- meeting with the DPO to decide where CCTV is needed to justify its means; and
- conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.

Purpose and justification

The school will only use surveillance cameras for the safety and security of the school and its staff, students and visitors. Surveillance will be used as a deterrent for violent behaviour and damage to the school. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any 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;
- 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.

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 Executive Headteacher and Designated Safeguarding Lead (DSL) 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 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
- urinals

Security measures are in place to prevent tampering with any of the camera's parameters, including location and viewing angle.

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 throughout the premises where the surveillance system is active, 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

Adequate security measures are in place to ensure security of footage and the integrity of the system. Specifics are not disclosed in this document, but are held internally.

Levels of protection may vary due to different specifications and ages of Digital Video Recording (DVR) equipment. 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;
- isolating CCTV equipment to the school IT network only;
- utilising different access levels (where supported);
- auditing access on recorders (where supported);
- locating DVRs in restricted and/or monitored areas;
- encrypting data on drives and during network transmission (where possible);
- physically obscuring and securing equipment such as DVRs, cabling and power supplies from general access (where possible);
- 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 Executive Headteacher, or in cases where this may prejudice the outcomes, the Chair of the Trust Board.

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 Head of School and the Data Controller are 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 DVRs.

Footage captured and stored on DVRs will be automatically overwritten at the end of the pre-determined retention period, which is set and stored internally.

Footage extracted from DVRs 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 SSMAT Data Protection (GDPR) Policy and Records Management (GDPR) Policy.

Access to, and disclosure of, recorded Images

Access to recorded images will be restricted to those authorised to view them, and will not be made publically available.

Access will not be granted to the system without a valid reason and will only be given after an appropriate risk assessment has been conducted.

Access to CCTV footage will not generally be permitted where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

Access may be restricted to coverage of specific relevant areas.

A register of individuals having access to the system will be held securely in the school, and will be subject to review.

Access is only to be carried out using school-owned and security compliant equipment.

Under GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All disks containing images belong to, and remain the property of, the school.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing, as detailed in the GDPR Policy.

All Subject Access Requests should be submitted on the SAR Form, available from the school website. Individuals submitting requests for access will be required to provide sufficient information to enable the footage relating to them to be identified. This will usually include date, time and location.

Information provided will be in an electronic format - either sent by secure email or on optical media (compact disc). The timeframe for providing this data is forty days from the SAR. This timeframe may be extended due to school closures (e.g. holidays or exceptional circumstances) by up to another calendar month. Further information can be found in the Data Protection (GDPR) Policy.

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 Head of School will decide whether recorded images may be released to persons other than the police, consulting with the Executive Headteacher and/or DPO, as required.

SJ/SM; 31/08/20