SAFE START SCHOOL

WILLPOWER-INITIATIVE-SUCCESS-EMPATHY

SafeStart School

Close Circuit TV (CCTV) Policy

Author	Grace Speakman - Acting Headteacher
Date Policy/ Guidance Written	October 2023
DFE Recommended Review Frequency	GB - Annually
Date of next review	January 2024
File Location	Staff Shared Drive General File / Policies
Details of dissemination of Policy/ Guidance (to who, date, method)	Staff at relevant meetings and through Line Management and Staff Appraisal. Governing Body Meetings

Contents

Statement of intent

At Safestart School, we take our responsibility towards the safety of students, staff, parents/carers, and visitors very seriously. To that end, we use close circuit TV 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 CCTV system 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 usable 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.

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 (Student 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
- Keeping Children Safe in Education 2021-23

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 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: Data protection code of practice for surveillance cameras/personal info'

Definitions

For the purpose of this policy a set of definitions will be outlined:

Surveillance – Monitoring the movements and behavior of individuals; this can include video, audio, or live footage. For the purpose of this policy only video footage will be applicable.
If sound is to be used, this will be under the directive of the School Data Protection Officer (DPO) and in liaison with the Company Proprietor.

Overt surveillance – Any use of surveillance for which authority does not fall under the Regulation of Investigatory Powers Act 2000. Overt surveillance footage will be clearly signposted around the school.

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.
Safestart School 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.

Company Proprietor	**Director- Rachel Pilling**
Chair of Governors	**Louise Nixon**
School's Data Protection Officer (DPO) / CCTV Data Controller	**Acting Headteacher – Miss Grace Speakman**

Roles and Responsibilities

Responsibilities for the school's security are shared between the Proprietor, Governing Body and Headteacher **The "Responsible Person" the School's Data Protection Officer (DPO) is the Headteacher.** This includes:

- Ensure appropriate signage regarding CCTV is displayed (externally and internally) • 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 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 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 highest management level of the school, e.g., the Governing Body.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Presenting reports regarding data processing at the school to the Governing Body.

Safestart School, as the corporate body, is the data controller. The Proprietor in liaison with the Governing Body of Safestart School therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Headteacher 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/CCTV footage legally and fairly.
- Collecting surveillance/CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance/CCTV footage that is relevant, adequate, and not excessive in relation to the reason for its collection.
- Ensuring surveillance/CCTV footage identifying an individual is not kept for longer than is necessary.

• Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure – especially when processing over networks.

The role of the Headteacher includes:

• Meeting with Senior Leaders to decide where CCTV is needed to justify its means.

• Conferring with Senior Leaders with regard to the lawful processing of the surveillance /CCTV footage.

• Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.

• Monitoring legislation to ensure the school is using surveillance fairly and lawfully.

• Communicating any changes to legislation with all members of staff, the Proprietor and Governing Body

The role of the Proprietor and members of the Governing Body includes:

• The Governing Body is responsible for formulating the CCTV Policy and monitoring its implementation.

• Conferring with the Headteacher with regard to the lawful processing of the surveillance /CCTV footage.

• Monitoring legislation to ensure the school is using surveillance fairly and lawfully.

Purpose and justification

The school will only use surveillance cameras for the safety and security of the school and its staff, students, parents/carers, 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 any changing facility. If the surveillance and CCTV systems fulfill their purpose and are no longer required, the school will deactivate them.

The Data Protection Principles / GDPR

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, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

• Adequate, relevant, limited to what is necessary in relation to 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 are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay.

• Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are 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.

Use of the CCTV System

The CCTV surveillance system will be used to:
• Maintain a safe environment.
• Ensure the welfare of students, staff, and visitors.
• Deter criminal acts against persons and property.
• Assist the police in identifying persons who have committed an offence.

Overview of the CCTV System

• The system comprises 19 fixed and dome cameras and they have all been professionally fitted.
• The CCTV is owned and operated by the school; the deployment of which is determined by the Headteacher in consultation with the Proprietor.
• CCTV advisory signs will be clearly and prominently placed.
• The CCTV is monitored centrally from the Headteacher office and stored in a lockable cabinet, monitored by the Data Controlling Officer (Headteacher).
• Changes to CCTV monitoring will be subject to consultation with staff and the school community.
• The school's CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018.
• 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 school data controller of their responsibilities under the CCTV Policy.
• All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

The CCTV is installed and is visible in the following locations:

- **GROUND FLOOR:**, Reception, KS4 Side Door
- **FIRST FLOOR:** Top of stairs, Hub,
- **SECOND FLOOR**:Games room
- **KS3 Building:** Central Area at top of the stairs, Teaching Floor, KS3 Kitchen

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.

Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.
The school's authorised CCTV system operators are:

- Acting Headteacher - Grace Speakman
- Senior Leader- Rachel Duffy – *As authorised by the* Data Controlling Officer (Headteacher).
- School Security- Emily Pilling- a*s authorised by the* Data Controlling Officer (Headteacher).

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies DfE *"Application for the use of directed surveillance"* guidance and protocols will be adhered to - authorisation forms will be completed and retained.
Surveillance and CCTV systems will be tested for security flaws annually to ensure that they are being properly maintained at all times.
Surveillance and CCTV systems will not be intrusive.
The Headteacher will decide when to record footage, e.g., a continuous loop will be recorded at each location. Any unnecessary footage captured will be securely deleted from the school system on a 30 day cycle.
Any cameras that present faults will be repaired immediately to avoid any risk of a data breach. The CCTV system can be accessed on the personal computers of the Headteacher, Operations manager and IT Support team by use of a password - *As authorised by the* Data Controlling Officer (Headteacher).

CCTV Code of practice

The school understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.
The school notifies all students, staff, parents/carers, and visitors of the purpose for collecting surveillance data via signs in the school grounds where cameras are based.
CCTV cameras are placed where they do not intrude on anyone's privacy and are necessary to fulfill their purpose. The Headteacher/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 students, students, parents/carers, 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 students, staff, parents/carers, 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 consider its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point who will be the **Data Protection Officer (DPO) / Data**

Controller, through which people can access information and submit complaints.

- Have clear responsibility/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.
- Be registered in line with Data Protection and all signs with QR codes will be accessible and show the schools details and information.

Access to Data

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All media containing images belong to, and remain the property of, the school. Individuals have the right to submit a Subject Access Requests (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied. A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. Requests by persons outside the school for viewing or obtaining digital recordings, will be assessed by the Headteacher / DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation. Close liaisons with the Proprietor will occur throughout.
Where a request is manifestly unfounded, excessive, or repetitive, a reasonable fee will be charged.
All fees will be based on the administrative cost of providing the information.
All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
If it is found that a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.
It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.
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 and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

Access to images by Third Parties

Requests for access to images will be made using the 'Application to access to CCTV images' form accompanied by a **£10.00 fee** (which is non-refundable if the request is declined).
The Data Controller will assess applications and decide whether the requested access will be permitted.
Release will be specifically authorised and agreed with the Proprietor.
Disclosure of recorded images to third parties will only be made in limited and prescribed circumstances.
E.G, in cases of the prevention and detection of crime, disclosure to third parties will be limited to the following: • Law enforcement agencies where the images recorded would assist in a specific criminal enquiry

- Prosecution agencies
- Relevant legal representatives
- The press/media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness, or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be considered.
- People whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings)

All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented as above.

Disclosure of Images to the Media

If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of other individuals must be disguised or blurred so that they are not readily identifiable. If the CCTV system does not have the facilities to carry out that type of editing, an editing company may need to be used to carry it out. If an editing company is used, then the data controller must ensure that there is a contractual relationship between them and the editing company, and:

- That the editing company has given appropriate guarantees regarding the security measures they take in relation to the images
- The written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the data controllers
- The written contract makes the security guarantees provided by the editing company explicit

Access by Data Subjects

This is a right of access, which is provided by section 7 of the 1998 Act. Requests for access to images will be made using the 'Application to access to CCTV images' form accompanied by a **£10.00 fee** (non-refundable if the request is declined).

Monitoring and review

This policy will be monitored and reviewed on a yearly basis, or in light of any changes to relevant legislation by the Headteacher. The Headteacher will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.
The Headteacher will communicate changes to this policy to all members of staff.

Complaints

Complaints and enquiries about the operation of CCTV within Safestart School should be directed to the Headteacher in the first instance.

Further Information

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

- The Information Commissioner's Office CCTV Code of Practice 2014
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018
- General Data Protection Regulation

APPLICATION FOR CCTV DATA ACCESS

ALL Sections must be fully completed. Attach a separate sheet if needed.

Name and address of Applicant	
Name and address of "Data Subject" – i.e., the person whose image is recorded	
If the data subject is not the person making the application, please obtain a signed consent from the data subject opposite	Data Subject signature……
If it is not possible to obtain the signature of the data subject, please state your reasons.	
State your reasons for requesting the image.	
Date on which the requested image was taken.	
Time at which the requested image was taken.	
Location of the data subject at time image was taken (i.e., which camera or cameras.)	
Full description of the individual, or alternatively, attach to this application a range of photographs to enable the data subject to be identified by the operator.	
Please indicate whether you (the applicant) will be satisfied by viewing the image only.	

On receipt of a fully completed application and the £10.00 nominal fee, a response will be provided as soon as possible, and in any event within 40 days. In the event of a declined application the fee is non-refundable.

SCHOOL USE ONLY	SCHOOL USE ONLY
Headteacher discussed with Proprietor	YES ❑ NO ❑ Date:
Access granted	YES ❑ NO ❑
If access **NOT** granted - Reason for not granting access:	

Data Controller's name: Signature: Date:	Proprietor name: Signature: Date: