



SAFE START SCHOOL

WILLPOWER-INITIATIVE-SUCCESS-EMPATHY-RESPECT

SafeStart School

Security Camera and Video/Audio Surveillance Policy

Author	Grace Speakman
Date Policy/ Guidance Written	October 2023
Reviewed date	October 2026
DFE Recommended Review Frequency	GB - Annually
Date of next review	October 2027
Policy Lead	Data Protection Lead/DPO
Approved by	Proprietor

Statement of intent

Safe Start School uses a security camera surveillance system to support the safety, security and safeguarding of students, staff, visitors and the school premises.

The surveillance system involves the processing of personal data. The school will therefore ensure that the surveillance system is operated lawfully, fairly, transparently and proportionately in accordance with applicable data protection legislation.

A security camera surveillance system will only be used where the school considers its use necessary and proportionate for clearly defined purposes.

The school will respect individuals' privacy and will not use the security system in areas where there is a reasonable expectation of privacy, such as toilets or changing facilities.

Terminology

Safe Start School operates security cameras as part of its security and safeguarding arrangements. For the purposes of this policy and data protection legislation, these cameras are treated as a video surveillance system.

References within this policy to “security cameras” or “the surveillance system” include the school's cameras and associated video and audio recording facilities.

Purpose of Security Camera Surveillance System

The surveillance system may be used to:

- support the safety and welfare of students, staff and visitors;
- support safeguarding arrangements;
- prevent and detect crime;
- deter violence, aggression, vandalism and damage;
- protect school buildings, equipment and property;
- assist with the investigation of incidents;
- support the investigation of safeguarding, disciplinary or other serious concerns where appropriate; and
- provide evidence to law-enforcement agencies where lawful and necessary.

Footage will not routinely be used for general monitoring of staff performance or conduct.

Legal Framework

This policy has regard to relevant legislation and guidance, including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Protection of Freedoms Act 2012;
- Human Rights Act 1998;
- Freedom of Information Act 2000, where applicable;
- Equality Act 2010;

- current Information Commissioner's Office guidance relating to video surveillance; and
- current statutory safeguarding guidance, including *Keeping Children Safe in Education*, where relevant.

The school will also have regard to the principles of the Surveillance Camera Code of Practice where applicable and relevant.

Data Controller and Responsibilities

Safe Start School/Safestart School Ltd is the data controller for personal data processed through the school's surveillance system.

The school's Data Protection Lead/DPO will provide advice and oversight in relation to data protection compliance.

The Headteacher/appropriate senior leader is responsible for the day-to-day operation of the surveillance system, including ensuring:

- cameras are used only for authorised purposes;
- access to footage is appropriately restricted;
- requests for footage are managed appropriately;
- security camera surveillance system signage remains in place;
- security measures are maintained;
- disclosures are appropriately authorised and recorded;
- retention arrangements are followed; and
- concerns or data breaches are appropriately reported.

Authorised users must comply with this policy and maintain confidentiality.

Lawful Processing and Data Protection Principles

Security camera footage will be processed in accordance with UK GDPR principles.

Personal data will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate where applicable;
- retained only for as long as necessary;
- appropriately protected against unauthorised or unlawful processing, loss, destruction or damage; and
- managed in a way that demonstrates accountability.

The school will identify and document an appropriate lawful basis for its surveillance system processing.

Security Camera Locations and Privacy

Cameras will only be positioned where their use is necessary and proportionate.

Cameras must not be installed in:

- toilets;
- changing facilities; or
- other areas where individuals would reasonably expect a high degree of privacy, except in genuinely exceptional circumstances where lawful, necessary and subject to appropriate assessment and authorisation.

Camera positioning should minimise unnecessary capture of neighbouring properties, public areas or other spaces outside the school's control.

The school should periodically review whether each camera remains necessary.

Audio Recording

The school's surveillance system records both video and audio within designated communal areas.

Security cameras are not installed in classrooms, staff rooms, offices, toilets, changing facilities or other areas where individuals would reasonably expect a higher degree of privacy.

Audio recording is used to support safeguarding and the safety of students, staff and visitors and, where necessary, to assist in establishing the context of serious incidents, including threats, aggression or other safeguarding concerns.

The school recognises that audio recording is more privacy intrusive than video surveillance alone. Its use will therefore be kept under review to ensure that it remains necessary and proportionate.

Clear signage and relevant privacy information will inform individuals that both video and audio recording are in operation.

Footage and audio will not be routinely accessed for general monitoring of staff performance or ordinary conversations.

Data Protection Impact

The school has completed a Data Protection Impact Assessment (DPIA) covering its security camera and video/audio surveillance arrangements.

The DPIA considers the necessity and proportionality of the surveillance system, including continuous audio recording, and the measures in place to protect the rights and privacy of students, staff and visitors.

The DPIA will be reviewed periodically and whenever there is a significant change to the surveillance system, including changes to camera locations, technology, recording capabilities or the purposes for which the system is used.

The continued necessity and proportionality of audio recording will form part of each review of the DPIA.

Signage and Transparency

Clear and appropriately positioned surveillance system signage will inform individuals that the surveillance system is in operation.

Signs should identify, as appropriate:

- that surveillance system is operating;
- the purpose of the surveillance;
- the organisation responsible for the system; and
- how further privacy information can be obtained.

Information about security camera surveillance system processing should also be reflected in the school's relevant privacy information/notices.

Access and Security

Access to live and recorded footage will be restricted to authorised individuals who require access for legitimate purposes.

The school will maintain appropriate technical and organisational security measures, including:

- secure accounts/passwords;
- access restrictions;
- appropriate device security;
- secure storage;
- appropriate control of downloaded/exported footage;
- confidentiality requirements; and
- periodic review of authorised users.

Authorised access should be reviewed when staff change roles or leave employment.

Where practicable, access to footage and disclosures should be logged.

Access through mobile or remote devices will only be permitted where authorised by the school and appropriate security controls are in place.

Retention

Recorded surveillance footage will normally be retained for up to 30 days, unless there is a legitimate reason to retain particular footage for longer.

Footage may be retained beyond the normal period where necessary, for example:

- for a safeguarding investigation;
- following an accident or incident;
- for disciplinary or grievance proceedings;

- in connection with a complaint;
- for legal proceedings;
- following a request from the police or another authorised body; or
- where a relevant access request has been received.

Footage retained for a specific purpose should be securely deleted when no longer required.

Viewing Surveillance Footage

Footage should only be viewed where there is a legitimate reason.

Where footage is viewed as part of an incident investigation, access should be limited to those who reasonably need to see it.

Staff must not:

- access the surveillance system or footage out of curiosity;
- show footage to unauthorised individuals;
- photograph, screen-record or otherwise copy surveillance footage using personal devices.
- share login details; or
- download or distribute footage without authorisation.

Unauthorised access, copying or disclosure may be treated as a data-protection breach and/or staff conduct matter.

Safeguarding and Surveillance

Surveillance footage may provide relevant evidence in relation to safeguarding concerns.

Where footage identifies or supports a safeguarding concern, staff must follow the school's Safeguarding and Child Protection Policy and report the matter appropriately.

A surveillance system does not replace appropriate staff supervision, safeguarding practice or professional vigilance.

Relevant footage should be preserved where required for safeguarding enquiries or investigations.

Disclosure to Third Parties

Security camera footage will only be disclosed where there is a lawful and legitimate reason.

This may include disclosure to:

- police or other law-enforcement agencies;
- safeguarding agencies;
- courts or legal representatives where appropriate;
- insurers;
- regulators; or

- individuals exercising their data-protection rights.

Before disclosure, the school will consider:

- the identity and authority of the requester;
- the purpose of the request;
- the lawful basis for disclosure;
- whether disclosure is necessary and proportionate;
- the rights and privacy of other individuals shown; and
- whether footage needs to be redacted or blurred.

A record should be maintained of significant disclosures.

Media

Security camera footage will not normally be released directly to the media.

Any proposed disclosure to the media must be authorised at an appropriate senior level and assessed carefully for lawfulness, necessity, proportionality, safeguarding and the privacy rights of individuals shown.

Where police are investigating an incident, any media release should normally be coordinated with the relevant law-enforcement agency.

Subject Access Requests

Individuals have the right to request access to their personal data, which may include footage containing their image.

Requests should be submitted to the school/DPO with sufficient information to identify the relevant footage, such as:

- date;
- approximate time;
- location; and
- information enabling the individual to be identified.

The school may need to verify the requester's identity.

Where footage contains other identifiable individuals, the school will consider whether it can appropriately disclose the footage, including whether redaction is required.

Requests will be handled in accordance with applicable data-protection legislation.

Requests from Police and Other Agencies

Requests from police or other agencies should be referred to the DPO/Data Protection Lead or authorised senior leader.

The school should establish:

- who is requesting the footage;
- the purpose of the request;
- the legal basis for disclosure;
- the specific footage required; and
- whether disclosure is necessary and proportionate.

Where appropriate, the request and disclosure should be documented.

Covert Surveillance

The school does not routinely undertake covert surveillance.

Covert surveillance will only be considered in exceptional circumstances where there is a compelling and lawful justification, less intrusive methods would not reasonably achieve the purpose, and appropriate senior and data-protection advice/authorisation has been obtained.

Any proposed covert surveillance must be subject to a documented assessment of necessity, proportionality, privacy and legal requirements before implementation.

Data Breaches

Any suspected loss, unauthorised access, disclosure, copying or misuse of security camera footage must be reported immediately in accordance with the school's data-protection breach procedure.

The DPO/Data Protection Lead will assess the incident and determine whether further action or notification is required.

Complaints

Complaints about the operation of the surveillance system should normally be raised with the Headteacher or DPO/Data Protection Lead.

Complaints will be considered in accordance with the school's complaints and data-protection arrangements.

Individuals also have the right to raise concerns with the Information Commissioner's Office where appropriate.

Monitoring and Review

The school will periodically review its security camera surveillance system arrangements to ensure that:

- cameras remain necessary and proportionate;
- camera positioning remains appropriate;
- signage remains accurate;
- authorised-user access remains appropriate;
- security measures remain effective;

- retention arrangements are being followed;
- the continued use of audio recording remains necessary, proportionate and appropriately controlled;
- relevant privacy information remains accurate; and
- The surveillance system continues to achieve its stated purposes.

This policy will be reviewed annually or sooner where there are significant changes to legislation, guidance, technology or the school's security camera surveillance system arrangements.