Surveillance and CCTV Policy

The CEO/COO will review this policy on a 2 yearly cycle

Policy Version:	V1
Colleagues affected by this Policy:	All stakeholders
Person responsible for the Policy:	COO
Approved by/ date:	CEO December 2025
Next review:	December 2027

Contents:

Statement of Intent

The Sea View Trust is committed to the safety of staff, visitors, and pupils. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our settings' and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at our settings' and ensure that:

- We comply with data protection legislation.
- 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; and
- Using images of individuals that could affect their privacy

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff, and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.
- To assist in the day-to-day management of staff, pupils, and visitors, including ensuring the health and safety of all individuals.
- To assist in the effective resolution of disputes which arise during disciplinary and grievance proceedings.
- To assist in the defence of any civil litigation, including employment tribunal proceedings.

Legal Framework

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

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004

- Equality Act 2010

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

- Biometrics and Surveillance Camera Commissioner (2022) 'Amended Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2022) 'Video Surveillance'
- DfE (2022) 'Protection of biometric data of children in schools and colleges

This policy operates in conjunction with the following school policies:

- SVT – GDPR SAR Procedure
- SVT – GDPR Data Protection Policy
- SVT – Privacy Notice

Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio, or live footage. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** - surveillance which is clearly visible and signposted around the premises and 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.

The Trust does not condone the use of covert surveillance when monitoring staff, pupils 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

The Sea View Trust is the data controller with overall responsibility and accountability for data protection compliance. Sea View Trust's trustees, as the highest level of management, have overall responsibility for compliance with all applicable law.

The role of The Sea View Trust includes:

- Meeting with the Data Protection Officer (DPO) to decide where CCTV is needed to justify its means and conveying this information to its settings.
- Conferring with the DPO with regard to the lawful processing of the surveillance and 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 settings in The Sea View Trust

The role of the **Trust Data Protection Officer (DPO)** - includes:

- Dealing with freedom of information requests and subject access requests (SAR) in line with legislation, including data protection legislation and the Freedom of Information Act 2000.
- Ensuring that guidance is provided to all staff to handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is procured in line with legal requirements.
- 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 Trust's level of risk related to data protection and processing performance.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.

The **Academy Business Leads, in collaboration with the Academy IT Technician** deals with the day to-day matters relating to the use of surveillance and CCTV within our settings.

The role of the Academy Business Leads and the Academy IT Technician includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and 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 longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration, and disclosure – especially when processing over networks.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Reporting any breaches of data protection legislation to the DPO in accordance with the Trust's Data Breach Policy.
- Reporting any subject access requests to the DPO in accordance with the Trust's GDPR Data Protection Policy.

Purpose and Justification

Each setting will only use surveillance cameras for the safety and security of the school and its staff, pupils, and visitors.

Surveillance will be used as a deterrent for violent behaviour and damage to the school.

Each setting will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in any changing facility. Under specific circumstances, CCTV may be installed in classrooms. Where this is the case, it will be well documents and notices will always be clear that CCTV is in use. If the surveillance and CCTV systems fulfil their purpose and are no longer required, the setting will de-activate them.

Data Protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals as determined by a data protection impact assessment (DPIA), or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests' assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and considering advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical 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 they are processed, is 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 is processed.
- 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

A DPIA will be carried out prior to the installation of any new surveillance, CCTV, or biometric system. The DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

Prior to introducing any new surveillance, CCTV, or biometric system, please contact the DPO for advice on completing the DPIA in accordance with the Trust's GDPR Data Protection Policy. If the DPIA reveals any

potential security risks or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues.

Where a setting identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the DPO before they use CCTV, and the Trust will act on the DPO's advice. In the event that the high risk to individuals cannot be mitigated, the DPO will liaise with the ICO and will comply with the ICO's advice.

Each setting 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 setting will seek amendments to the use of the surveillance.

Surveillance and CCTV systems will not be intrusive. Pupils, staff, and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose, and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

Biometric technology will not be entered into without the consent of The Sea View Trust as there are specific legal requirements to obtain consent from parents prior to obtaining biometric data from children.

Objectives

The surveillance system will be used to:

- Ensure the welfare of pupils, staff, and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.
- Maintain a safe environment.
- To assist in the day-to-day management of staff, pupils, and visitors, including ensuring the health and safety of all individuals.
- To assist in the effective resolution of disputes which arise in the course of disciplinary and grievance proceedings.
- To assist in the defence of any civil litigation, including employment tribunal proceedings

Protocols

The surveillance system will be registered with the ICO by The Sea View Trust, in line with data protection legislation.

The main surveillance systems used are closed digital systems which in some circumstances may record sound.

Warning signs will be placed throughout the premises where the surveillance system is active, as mandated by the ICO's CCTV and Video Surveillance Guidance. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

Surveillance systems within our settings have been designed for maximum effectiveness and efficiency; however, each setting 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 each setting, unless monitoring car parking areas for security purposes.

Security

Access to the surveillance system, software and data will be strictly limited to authorised operators and will be password protected.

Authorised CCTV system operators are limited to those who need to gain access at each setting and may include:

- Headteacher/Head of School
- Business Lead
- Trust Business Leads
- Chief Operating Officer
- IT Technician
- Trust IT Manager
- Site Supervisor
- Admin Team
- DPO Forbes Solicitors

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 of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will not be intrusive.

The Academy Business Lead will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

Any unnecessary footage captured will be securely deleted from the settings' system.

Any cameras that present faults will be repaired immediately, or as soon as is reasonably practicable, to avoid any risk of a data breach.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

Each system will have a separate audio and visual system that can be run independently of one another. The school will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording;
- Considered other less privacy intrusive methods of achieving this need;
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording.

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.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

Surveillance footage will be held for security purposes however, each setting in the Trust may have differing lengths of time which footage will be retained; this will not exceed 60 days. The Academy IT Technician and the Academy Business Leads are responsible for keeping the records secure and allowing access. When no longer required, all images stored in whatever format will be erased permanently and securely. Any physical matter such as tapes or discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

The surveillance and CCTV systems are owned by The Sea View Trust and images from the system are strictly controlled and monitored by authorised personnel only.

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

This policy is available on the Trust's website. Each setting notifies all pupils, staff, and visitors of the purpose for collecting surveillance data via various means including notice boards, signs, letters, and email.

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, 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.
- 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 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 pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up to date.

Access

Under the data protection legislation, 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 Trust.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data to verify the lawfulness of the processing.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for.
- The Trust is relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
- The data has been processed unlawfully.
- There is a specific legal obligation.

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority.
- Certain research activities.
- Compliance with a specific legal obligation.

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by the Trust or object to way it was processed.
Data can be restricted by either:

- Moving the data to another processing system.

- Making the data unavailable to users.

Any subject access requests or requests for erasure must be forwarded to the DPO in accordance with the Trust's GDPR Data Protection Policy and the Trust's SAR Procedure.

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) or the Health and Safety Executive (HSE).
- Relevant legal representatives – such as lawyers and barristers.
- Insurers
- Department for Education (DfE)
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation.

Requests for access or disclosure must be recorded and forwarded to the DPO for advice. The Headteacher/Head of School of the setting concerned will make the final decision as to whether recorded images may be released to persons other than the police in accordance with guidance provided by the DPO.

Monitoring and review

This policy will be monitored and reviewed on an annual basis by the Data Protection Officer (DPO) and the Chief Operating Officer (COO) in conjunction with the Trust IT Manager (ITM).

The COO in conjunction with the Trust IT Manager (ITM) will be responsible for monitoring any changes to legislation that may affect this policy and make the appropriate changes accordingly.

The Headteacher/Head of School of each setting will communicate changes to this policy to all members of staff.

Related policies and procedures

GDPR Data Protection Policy

SAR Procedure

Data Retention Schedule

Appendix 1 - Authorised CCTV Operators

NAME	POSITION	DATE ADDED	DATE REMOVED	NOTES

Appendix 2 - Request for CCTV Images

This form should be used for routine requests for access to view CCTV images by individuals whose images have been captured and/or uniformed police in response to incidents which occurred on the same day e.g. to assist in a specific criminal enquiry, identify a victim, witness, or perpetrator in relation to a criminal incident.

This form should **not** be used where the police or other law enforcement agencies request a *copy* of CCTV images. A Section 29 request should be made under the Data Protection Act 1998 for this type of access.

This form should **not** be used where an individual whose image has been recorded requests a *copy* of CCTV images relating to themselves. A subject access request under the General Data Protection Regulation (GDPR) 2018 is required for this type of access.

To be completed by Applicant:

Date	
Person making request	
Organisation	
Reason for request	
Crime reference number	

To be completed by a Sea View Trust Representative:

Reason for allowing access/disclosure	
Reason for refusing access/disclosure	
Name & Signature	
Position	
Date	