CCTV and Surveillance Policy

Document Details	
Category:	Risk and Health & Safety
Approved By:	Audit and Risk Committee
Version:	3
Status:	Approved
Issue Date:	April 2021
Next Review Date:	Summer Term 2022
Signed:	

Ownership and Control

History

Version	Author	Dated	Status	Details
1	BMa	March 2018	Approved	Board Meeting of 21 Mar 2018
2	KHo/JEl	July 2019	Approved	Annual review
3	JEL	April 2021	Approved	Annual review

Contents:

Statement of intent

At The Sigma Trust, we take our responsibility towards the safety of staff, visitors and pupils 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 CCTV systems at the school and ensure that:

- We comply with the GDPR.
- 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
- Using images of individuals that could affect their privacy

1. Legal framework

1.1. 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

1.2. 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 the 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: A data protection code of practice for surveillance cameras and personal information'

1.3. This policy operates in conjunction with the following Trust policies:

- Photography and Videos at School Policy
- E-security Policy
- Freedom of Information Policy
- School Security Policy
- Data Protection Policy

2. Definitions

2.1. 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** – 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.

2.2. The Sigma Trust does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

2.3. Any overt surveillance will be clearly signposted around the school.

3. Roles and responsibilities

3.1. 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 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 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.
- Reporting to the highest management level of the Trust, e.g. the Board of Trustees.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.

- Monitoring the performance of the Trust's data protection impact assessment (DPIA), and providing advice where requested.

3.2. The Sigma Trust, as the corporate body, is the data controller. The Board of Trustees of The Sigma Trust therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

3.3. The Local Governance Committee will ensure that by adoption of this policy they will support the Board of Trustees fulfil their legal obligations specified in 3.2.

3.4. The school's Data Manager deals with the day-to-day matters relating to data protection within their school and thus, for the benefit of this policy, will act as the data controller.

3.5. The role of the data controller 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.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.

3.6. The role of the headteacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Monitoring legislation to ensure the Trust is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4. Purpose and justification

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

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

4.3. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in general classrooms or any changing facility.

4.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them.

5. The data protection principles

5.1. 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 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 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.

6. Objectives

6.1. 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.

7. Protocols

7.1. The surveillance system will be registered with the ICO in line with data protection legislation.

7.2. The surveillance system is a closed digital system which does not record audio.

7.3. Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

7.4. 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.

7.5. The surveillance system will not be trained on individuals unless an immediate response to an incident is required.

7.6. The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

8. Security

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

8.2. The school's authorised CCTV system operators are cited in Appendix A.

8.3. The school staff authorised to record and retain images are cited in Appendix A. This appendix is to be completed locally for each Sigma Trust school.

8.4. The school staff authorised to access audio records are cited in Appendix A. This appendix is to be completed locally for each Sigma Trust school.

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

8.6. 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.

8.7. Surveillance and CCTV systems will be tested for security flaws once every month to ensure that they are being properly maintained at all times.

8.8. Surveillance and CCTV systems will not be intrusive.

8.9. Any unnecessary footage captured will be securely deleted from the school system as specified in this policy.

8.10. Each system will have a separate audio and visual system that can be run independently of one another. Audio CCTV will only be used in the case of deterring

aggressive or inappropriate behaviour and will be subject to additional security and access rights.

8.11. Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

9. Privacy by design

9.1. The use of surveillance cameras and CCTV will be critically analysed using a DPIA

9.2. A DPIA will be carried out prior to the installation of any surveillance and CCTV system.

9.3. If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

9.4. Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

9.5. The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

9.6. If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek alternative provision.

10. Code of practice

10.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

10.2. The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and signage.

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

10.4. All surveillance footage will be kept for two months for security purposes; the headteacher and the Data Manager are responsible for keeping the records secure and allowing access.

10.5. 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, pupils and visitors.

10.6. The surveillance and CCTV system is owned by the Trust and images from the system are strictly controlled and monitored by authorised personnel only.

10.7. The school 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. The policy is available from the school's website.

10.8. 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 pupils, staff and volunteers, and law enforcement.

10.9. Be accurate and well maintained to ensure information is up-to-date.

11. Access

11.1. Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

11.2. All disks containing images belong to, and remain the property of, the Trust.

11.3. Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

11.4. The Trust will verify the identity of the person making the request before any information is supplied.

11.5. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

11.6. Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

11.7. Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the headteacher, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.

11.8. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

11.9. All fees will be based on the administrative cost of providing the information.

11.10. All requests will be responded to without delay and at the latest, within one month of receipt.

11.11. 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.

11.12. Where 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.

11.13. 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.

11.14. 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.

11.15. Instances of access to recordings will be recorded in a log which can be produced on demand to the DPO, an authorised manager or Auditor/ Regulator and will be a complete record of access activity (Appendix B). This log should state:

- Dates of access,
- the period and location covered by the recording,
- the reason for access and

- name, position and authority of those who have accessed recordings
- whether or not copies were made

11.16. 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

11.17. 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.

12. Monitoring and review

12.1. This policy will be monitored and reviewed on an annual basis by the DPO and the headteacher.

12.2. The DPO will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

12.3. The headteacher will communicate changes to this policy to all members of staff.

12.4. The scheduled review date for this policy is summer term 2022.

APPENDIX A: Authorised Users Log

TO BE COMPLETED LOCALLY FOR EACH INDIVIDUAL SIGMA TRUST SCHOOL

Name of School: _____

AUTHORISED CCTV SYSTEM OPERATORS	
Name	Job Title
STAFF AUTHORISED TO RECORD AND RETAIN IMAGES	
STAFF AUTHORISED TO ACCESS AUDIO RECORDS (Headteacher only)	

Signed:

Headteacher: _____ Date: _____

Chair of Governors: _____ Date: _____

APPENDIX B: Surveillance recordings Access Request Form: Investigators

Any transaction which sees information about individuals managed by the Trust leave the custody of authorised staff must be recorded so that we can evidence that such transfers were done lawfully. As such this form should be completed in every instance of surveillance recordings being transferred to a representative of another organisation who is authorised to receive them.

Section 1
Where you know the identity of a person or persons who are the subject(s) of your request, you should supply these details. This can be completed by our employees at the time of receiving the request.

Section 2
The request should be limited to specific locations and times to ensure that the information supplied is not excessive and to assist us in managing requests effectively. This can be completed by our employees at the time of receiving the request.

Section 3
The person receiving copies of surveillance recordings or still images must state who they are, their position within their organisation and the name of their organisation. They must sign at the point of receiving the information to confirm that are authorised to receive it and that the organisation that they represent conforms to Data Protection law and will accordingly safeguard the data.

Section 4
An authorised person for us should state what has been provided; in what format the information has been supplied (e.g. tape, disc, USB Memory stick, printed still images, etc.) and the quantity. We should also confirm by signature that the request has been fulfilled according to our procedures and that the information has been taken by the named person in section 3.

Surveillance recordings Access Request Form: Investigators

Please complete this form with the relevant details to enable us to successfully process your request

1. Personal details of the person to whom the request relates (The 'Data Subject') if known:				
Mr/Mrs/Miss:	First Name(s):			Surname:
Present address:				
Gender:				Date of Birth:
Male	☐	Female	☐	

2. Details of the information required:	
Please provide us with accurate information about the images you wish to view	
Date(s):	Time(s):
Location:	
Description of Incident:	

3. Declaration of the person authorised to receive CCTV copy recordings		
Mr/Mrs/Miss:	First Name(s):	Surname:
Working for Organisation (e.g. Essex Police Authority):		Position:
I confirm that the Surveillance copy recordings I have received will be handled according to the principles of the Data Protection Act 2018/ General Data Protection Regulations 2016		☐
Signed:		Date:

4. Approval by us and confirmation of handover of surveillance copy recordings	
I confirm that the following items and quantities were given into the custody of the above named person	☐
I confirm that surveillance copy recordings were received by the above named authorised person on the date below and relate only to the times and locations stated in the request.	☐
I confirm that this activity will be recorded on the Surveillance Equipment Access Log	☐
Signed:	Date:

The Sigma Trust is committed to the principles of the Data Protection Act 2018 and General Data Protection Regulations (2016). As such the information you have supplied on this form will be used only for the purposes of managing this access request.

APPENDIX C: CCTV Access Log

TO BE COMPLETED LOCALLY FOR EACH SCHOOL

Date of Access	Equipment Ref	Equipment Type	Date of Recording	Time of Recording		Reason for Access	Name of Employee (Access)	Name of Employee (Approve)	Copies made?	Method of Transfer	3rd Parties Present?	3rd Party data removed?	3rd Party Investigation Form
				From	**To**								

APPENDIX D: CCTV Impact Assessment and Review

Building/ Location					
Site Reference			Camera Ref		
System Owner			Signage in place?	☐	
Viewing Internal	☐		Viewing Private Area (Staff Only)	☐	
Viewing External	☐		Viewing Public Area	☐	
Date of Assessment			Date of Next Review		
Equipment Check Date (Last)			Equipment Check Date (Next)		
Declared Purposes					
Building Security	☐		Prevention of crime	☐	
Safety of Staff/ Public	☐		Detection of crime	☐	
Statistical data gathering	☒				

Considerations	
Alternatives to CCTV have been considered and rejected	☐
Wider uses of CCTV data have been considered but the declared purposes are restricted to the above	☐

Level of Image Quality Required		
☐	**Monitoring**	No need to identify individuals amongst general people traffic
☐	**Detecting**	Need to detect the presence of a person but not to see their face
☐	**Recognising**	Need to differentiate between people known to staff and those not
☒	**Identifying**	Need to establish someone's identity beyond reasonable doubt

Period of Activity			
24/7 x 365 days	☐	Seasonal/ Fixed term	☐
Specific Days	☐	Specific Times of Day	☐
Clarification (specify periods if not 24/7 x 365 days)			

Compliance with Policy	
System Owner understands their responsibilities in relation to Policy in the following areas: (tick to acknowledge)	
Restrict Access to individuals trained in CCTV procedures and authorised by you	☐
Log all instances of accessing recordings	☐
Release data only through use of approved requests	☐
Inform Access to Records and Information Champion of all requests for data	☐
No recorded data to be held beyond retention period stated in CCTV Policy	☐
Inform Information Champion immediately of any information security breaches	☐
Maintain methods of advising that CCTV cameras are present (e.g. signage)	☐
Annual reviews to be undertaken of necessity for CCTV cameras	☐

Signature				
System Owner		Date		
Approver		Date		
Decision	Approved		Declined	