ELMS FARM PRIMARY SCHOOL CCTV POLICY

THIS DOCUMENT IS a statement of the aims, principles and procedures for the use of CCTV at Elms Farm Primary School.
IT WAS DEVELOPED in September 2018
IT WAS APPROVED by the governing body in 2018.
REVIEWED: March 2022. September 2023, September 2025.

Our School Values

Ambition: We are ambitious for every child to achieve their best and be ambitious about their learning and their future.

Community: We value everyone in our community and learn how to look after each other and our environment. We respect each other and work together.

Equality: We value each other, our beliefs and differences are celebrated. Everyone is treated equally and fairly.

We are a Rights Respecting School
This policy links to the UN Convention for the right of the child:

At Elms Farm Primary School, 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 UK 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

ELMS FARM PRIMARY SCHOOL CCTV POLICY

The CCTV system used by the school comprises of fixed Samsung cameras, model QNR-6010R in the following locations:

Infants:

CH	Video	Audio	Camera Name
1	ON	OFF	EYFS Garden
2	ON	OFF	EYFS Gate
3	ON	OFF	Yellow Garden
4	ON	OFF	Infants Garden
5	ON	OFF	Infants Gazeebo
6	ON	OFF	Infants Canopy
7	ON	OFF	Infants Gate
8	ON	OFF	Infants Ent
9	ON	OFF	Nursery Canopy
10	ON	OFF	Nursery Garage
11	ON	OFF	Entrance Path
12	ON	OFF	Main Entrance
13	ON	OFF	Kitchen Carpark
14	ON	OFF	Reception
15	ON	OFF	CAM 15
16	ON	OFF	CAM 16

Juniors:

CH	Video	Audio	Camera Name
1	ON	OFF	Boiler House
2	ON	OFF	KS2 Carpark
3	ON	OFF	Lower Play Left
4	ON	OFF	Lower Play Mid1
5	ON	OFF	Lower Play Mid2
6	ON	OFF	Juniors Gazeebo
7	ON	OFF	Mid Playground
8	ON	OFF	PlaygroundHall1
9	ON	OFF	PlaygroundHall2
10	ON	OFF	EYFS Garden
11	ON	OFF	House Front
12	ON	OFF	House Rear
13	ON	OFF	By Juniors Toilets
14	ON	OFF	Y5/Y6 Landing
15	ON	OFF	Y3/Y4 Landing
16	ON	OFF	CAM 16

ELMS FARM PRIMARY SCHOOL CCTV POLICY

1.0 LEGAL FRAMEWORK

1.0 This policy has due regard to all relevant 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 (GDPR)
- Data Protection Act 2018
- 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
- School Standards and Framework Act 1998
- Children Act 1989
- Children Act 2004
- Equality Act 2010

1.1 This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office (2021) 'The Surveillance Camera Code of Practice'
- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

2.0 DEFINITIONS

For the purpose of this policy the following definitions are given for the below terms:

- Surveillance – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings. 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 school 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 school 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.

ELMS FARM PRIMARY SCHOOL CCTV POLICY

3.0 R0LES & RESPONSIBILITIES

The role of the DPO includes:

- Dealing with freedom of information requests and SARs 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 UK 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 highest management level of the school, e.g. the governing board.
- 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.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

The school, as the corporate body, is the data controller. The governing board 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.

3.2 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.

3.3 The headteacher is responsible for:

- 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.
- 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.

4.0 **PURPOSE**

Review of this policy shall be repeated regularly, and whenever new equipment is introduced, a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the school in reaching these objectives:

(a) To protect pupils, staff and visitors against harm to their person and/or property.

(b) To increase a sense of personal safety and reduce the fear of crime.

(c) To protect the school buildings and assets.

(d) To support the police in preventing and detecting crime.

(e) To assist in identifying, apprehending and prosecuting offenders.

(f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence

(g) To assist in managing the school.

5.0 DATA PROTECTION

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner.
- 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.

The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.

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

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.

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.

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 amendments.

Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the use of CCTV on site.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 3 weeks.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than is necessary.

6.0 SYSTEM MANAGEMENT

6.1 Access to the CCTV system and data shall be password protected and will be kept in a secure area.

6.2 The CCTV system will be administered and managed by the site Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the system will be managed by the Headteacher.

6.3 The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

6.4 The CCTV system is designed to be in operation 24 hours a day, 365 days a year, though the school does not guarantee that it will be working during these hours.

6.5 The System Manager will The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that the cameras are functional.

6.6 Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images. Images produced by the equipment must be as clear as possible so that they are effective. To achieve this, we will ensure that:
(a) the equipment is properly installed, serviced, checked and maintained (and maintenance logs maintained) to ensure it works properly;
(b) any recording media, if needed, will be of good quality and will be replaced if the quality of the images has begun to deteriorate;
(c) where time/date of images are recordable, the equipment will be set accurately and this will be regularly checked and documented;
(d) cameras will be correctly positioned;
(e) assessments will be made as to whether constant real-time recording is necessary, or if recording can be limited to those times when suspect activity is likely to occur;
(f) cameras will be protected from vandalism so far as is possible; and
(g) if cameras break down or are damaged, the [IT department] is responsible for arranging timely repair.

6.7 Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

6.8 Where a person other than those mentioned above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

6.9 Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

7.0 DOWNLOADING CAPTURED DATA ONTO OTHER MEDIA

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

(a) Each downloaded media must be identified by a unique mark.
(b) Before use, each downloaded media must be cleaned of any previous recording.
(c) The System Manager will register the date and time of downloaded media insertion, including its reference.
(d) Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.
(e) If downloaded media is archived the reference must be noted.
(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

7.2 Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

7.3 A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

7.4 Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of the school, and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the downloaded media (and any

images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

7.5 The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

7.6 Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the school's Data Protection Officer and a decision made by a senior leader of the school in consultation with the school's Data Protection Officer.

8.0 REQUESTS FOR ACCESS BY THE DATA SUBJECT

8.1 The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Headteacher.

8.2 Please refer to our Data Protection Policy with Subject Access Request appendix for further details.

8.3 If we cannot comply with the request, the reasons for not being able to comply will be documented and the data subject will be advised of these in writing.

8.4 The assigned manager responsible for the CCTV system will liaise with the Data Protection Officer, Judicium Consulting, and the school's Designated Safeguarding Lead to determine whether disclosure of the images will reveal third-party information, to assess the risks involved with disclosure and the reasonableness in disclosure.

8.5 Particular care should be exercised when images of other people are included in the materials for disclosure. Images of other individuals will, if possible, be redacted unless there would be an expectation that their images would be released in such circumstances. Non-disclosure will be appropriate in most circumstances. If there is any doubt about what information must be provided to enquirers, please contact the school's Data Protection Officer, Judicium Consulting.

8.6 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.

8.7 In the event of numerous or complex requests, the period of compliance will be extended by no more than an additional 20 working days. 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.

8.8 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.

8.9 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.

8.9.1 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.

9.0 COMPLAINTS ABOUT CCTV

Any complaints in relation to the school's CCTV system should be addressed to the Headteacher, using the Complaints Policy.