High View Primary School

Opportunities to Thrive

CCTV Policy

To include the Data Protection Impact Assessment for CCTV

Spring Term 2025

Date of review: Spring Term 2028

CCTV POLICY

Introduction

The school recognises that CCTV systems can be privacy intrusive.

For this reason, the school has carried out a data protection impact assessment with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the data protection impact assessment has informed the school's use of CCTV and the contents of this policy.

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.

Objectives

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.

Purpose Of This Policy

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at the school. The CCTV system used by the school comprises of:

Camera Number	CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL / FIXED
1	Outdoor camera	Main entrance gate	N	Y	F
2	Outdoor camera	High level. Looking over gate 3 and 4.	N	Y	F
3	Outdoor camera	High level. Looking over EYFS playground	N	Y	F
4	DOME	Under shelter. looking over EYFS playground	N	Y	F

5	DOME	Under shelter. Looking over Nursery playground and entrance gate	N	Y	F
6	Dome	Corner of kitchen. looking over Nursery sheds and climbing area	N	Y	F
7	External bullet	Fire exit by P/Arts room and hall	N	Y	F
8	External bullet	Hall fire exit	N	Y	F
9	External bullet	Fire exit by ELSA. Also looking at quiet area	N	Y	F
10	External bullet	Looking in to KS1 playground back towards cabin	N	Y	F
11	External bullet	Looking over KS1 playground and climbing wall	N	Y	F
12	External bullet	Looking over basketball court and cabin	N	Y	F
13	External bullet	Looking into car park	N	Y	F
14	DOME	Reception	N	Y	F
15	Dome	Internal EYFS corridor outside Rabbits	N	Y	F
16	DOME	Internal corridor outside nursery	N	Y	F
17	Dome	Internal corridor outside hall and toilets	N	Y	F
18	Dome	Bottom of stairs near ELSA	N	Y	F
19	Dome	Internal outside ELSA	N	Y	F
20	Dome	In ELSA room	N	Y	F
21	Dome	Lower KS2 Corridor	N	Y	F
22	Dome	Bottom of stairs near gas cupboard	N	Y	F

23	Dome	ILA(currently not working)	N	Y	F
24	Dome	Top of stirs by Spanish room	N	Y	F
25	Dome	Upper KS2 corridor. Outside Kestrels	N	Y	F
26	Dome	Upper KS2 stairs	N	Y	F
27	Dome	Cabin	N	Y	F
28	Outdoor Bullet	Orchard entrance and gate 1	N	Y	N
29	Outdoor Bullet	Astro	N	Y	N
30	Dome	ILA	N	Y	N
31	Dome	Upper KS2 corridor	N	Y	N
32	Outdoor bullet	Cabin Playground	N	Y	N

Statement Of Intent

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements of both the Data Protection Act and the most recent Commissioner's Code of Practice.

The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

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 30 days.

System Management

Access to the CCTV system and data shall be password protected.

The CCTV system will be administered and managed by the Premises 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.

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

The CCTV system is designed to be in operation 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.

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

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by providing clear, usable images.

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.

Where a person other than those previously mentioned (Systems Manager, Headteacher, SLT), requests access to the CCTV data or system, the Headteacher and GDPR Lead/DPO must satisfy themselves of the identity and legitimacy of the purpose of any person making such a request. Where any doubt exists access will be refused.

Details of all visits and visitors accessing the CCTV system for any purpose, will be recorded in a system log (see appendix 1) including time/date of access and details of images viewed and the purpose for doing so.

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 and Headteacher or GDPR Lead/DPO, 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.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, 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.

A record will be maintained (system log) of the viewing or release of any downloaded media to the police or other authorised applicants.

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.

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.

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 Headteacher of the school in consultation with the school's data protection officer (Judicium).

Complaints About The Use Of CCTV

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

Request For Access By The Data Subject

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 GDPR Lead (in consultation with the Headteacher).

Public Information

Copies of this policy will be available on the school website or by request to the school office.

Appendix 1

CCTV Monitoring log

Images will be retained for 30 days unless requested as part of an incident and then stored on an encrypted flash drive, sealed and stored in the safe for the period of the investigation process or for 12 months whichever is the lesser.

Anyone, other than authorised SLT, looking at CCTV needs to have a specific reason and a second person with them. They must then jointly complete this form.

Date	Time	Name	Name	Reason/Purpose/Images

Appendix 2

High View Primary School

Opportunities to Thrive

Data Protection Impact Assessment (CCTV)

High View Primary School operates a CCTV system. As such High View Primary must consider the privacy implications of such a system. The completion of the Data Protection Impact Assessment (DPIA) highlights some of the key implications.

A Data Protection Impact Assessment is also recommended by the Surveillance Camera Code of Practice which sets out the guiding principles that should be applied when CCTV systems are in place to ensure that privacy risks are minimised whilst ensuring the aims of the CCTV system are met.

The Data Protection Impact Assessment looks at the wider context of privacy taking into account Data Protection Law and the Human Rights Act. It considers the need for the CCTV system and the impact it may have on individual privacy.

The Data Protection Impact Assessment helps determine whether the proposed system can be justified as proportionate to the needs of the school. In undertaking this Data Protection Impact Assessment High View Primary has considered its obligations under Data Protection Law.

The school recognises that it is good practice to undertake a Data Protection Impact Assessment annually, or when a system is altered or replaced in any way, and review the CCTV Policy in line with this assessment. A Data Protection Impact Assessment will typically consist of the following key steps:

1. Identify the need for a DPIA.
2. Describe the information flow.
3. Identify data protection and related risks.
4. Identify data protection solutions to reduce and eliminate the risks.
5. Sign off the outcomes of the DPIA

1. Identify the needs for a DPIA
Explain broadly what project aims to achieve and what type of processing it involves. Summarise why you identified the need for a DPIA.
What is the aim of the project? – CCTV consistently delivers benefits in terms of improved health and safety and security within schools. It complements other security measures which are in place within the school. CCTV aims to achieve the following: ● Improve the health and safety and security of pupils, staff, and visitors ● Protect the school buildings and internal infrastructure ● Improve pupil behaviour

- Reduce vandalism and unauthorised access to the buildings
- Provide assistance in the detection and prevention of crime

Parents have the assurance that their children are safe whilst in school. Parents are aware that with CCTV there is the potential for behaviour at school to improve. The Board of Governors are also of the opinion that this is the case.
The Privacy Notice highlights what personal information is used and the lawful basis for using this personal information. It also highlights who the school will share the personal information with and how long the information will be kept. The Privacy Notice documents what rights an individual has regarding their personal information. Reference is made to the CCTV system in the school's Information Asset Register.

2. Describing the Process					
Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? What types of processing identified as likely high risk are involved?					
Camera Number	**CAMERA TYPE**	**LOCATION**	**SOUND**	**RECORDING CAPACITY**	**SWIVEL / FIXED**
1	Outdoor camera	Main entrance gate	N	Y	F
2	Outdoor camera	High level. Looking over gate 3 and 4.	N	Y	F
3	Outdoor camera	High level. Looking over EYFS playground	N	Y	F
4	DOME	Under shelter. looking over EYFS playground	N	Y	F
5	DOME	Under shelter. Looking over Nursery playground and entrance gate	N	Y	F
6	Dome	Corner of kitchen. looking over	N	Y	F

		Nursery sheds and climbing area			
7	External bullet	Fire exit by P/Arts room and hall	N	Y	F
8	External bullet	Hall fire exit	N	Y	F
9	External bullet	Fire exit by ELSA. Also looking at quiet area	N	Y	F
10	External bullet	Looking in to KS1 playground back towards cabin	N	Y	F
11	External bullet	Looking over KS1 playground and climbing wall	N	Y	F
12	External bullet	Looking over basketball court and cabin	N	Y	F
13	External bullet	Looking into car park	N	Y	F
14	DOME	Reception	N	Y	F
15	Dome	Internal EYFS corridor outside Rabbits	N	Y	F
16	DOME	Internal corridor outside nursery	N	Y	F
17	Dome	Internal corridor outside hall and toilets	N	Y	F
18	Dome	Bottom of stairs near ELSA	N	Y	F
19	Dome	Internal outside ELSA	N	Y	F
20	Dome	In ELSA room	N	Y	F
21	Dome	Lower KS2 Corridor	N	Y	F
22	Dome	Bottom of stairs near gas cupboard	N	Y	F
23	Dome	ILA(currently not working)	N	Y	F
24	Dome	Top of stirs by Spanish room	N	Y	F
25	Dome	Upper KS2 corridor. Outside Kestrels	N	Y	F
26	Dome	Upper KS2 stairs	N	Y	F
27	Dome	Cabin	N	Y	F

28	Outdoor Bullet	Orchard entrance and gate 1	N	Y	N
29	Outdoor Bullet	Astro	N	Y	N
30	Dome	ILA	N	Y	N
31	Dome	Upper KS2 corridor	N	Y	N
32	Outdoor bullet	Cabin Playground	N	Y	N

3. Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

The CCTV system was installed in 09/09/2023.

The system has 32 cameras. If the School is looking to upgrade its system with additional cameras any decisions to install and expand the CCTV system must be agreed by the Board of Governors. This will be communicated to parents and pupils via the school's CCTV Privacy Notice. This will be published on the school website.

4. Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

What is the lawful basis for processing? – The lawful basis for processing is contained in the school's Privacy Notice.
The lawful basis includes the following:

- Article 6 and Article 9 (Special Category Data) under Data Protection Law
- The Common Law Duty of Care
- Health and Safety at Work Act
- Safeguarding Vulnerable Groups Act
- Working together to Safeguard Children Guidelines (DfE)

Does the processing achieve your purpose? – Cameras are located in areas where pupils and staff have access. Cameras are not located in areas where privacy is expected.

Is there another way to achieve the same outcome? – To support school security a Critical Incident Policy has been adopted (all external gates are locked and secured by 8.55am and not unlocked until 3.15pm) along with improved lighting and other improvements have been put in place.

How will you prevent function creep? – The lawful basis for processing will be contained in the school's Privacy Notice (CCTV). Where there have been material changes to the way CCTV is used, the school will undertake a review of its CCTV system to ensure compliance and mitigate against 'function creep.'

How will you ensure data quality and data minimisation? – Consider the source of the data. The school has a data retention policy which identifies data retention periods for CCTV. The school will continue to be compliant with its CCTV Policy and keep an up to date system log.

What information will you give the individuals? – The school will inform pupils, staff and visitors that CCTV is in use by installing signs, along with a contact telephone number.

How will you help them support their rights? – The school has a Subject Access Request procedure in place to ensure compliance with Data Protection Law. CCTV signage states a contact telephone number. The school will continue to be compliant with its Data Protection Policy.

5. Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	*Minimal, significant or severe*	*Low, medium or high*
Positioning of CCTV cameras at entrance points to the school and the issue of privacy	Remote	Minimal	**Low**
Housing of CCTV cameras outside and ingress of water	Possible	Significant	**Medium**
Ongoing maintenance of CCTV equipment preventing breakdowns, etc	Possible	Significant	**Medium**
CCTV policies and procedures not in place leading to inconsistencies, etc	Probable	Significant	**Low**
Appropriate CCTV signage in place which conforms to industry standards	Possible	Minimal	**Low**
Training not undertaken by those using CCTV	Possible	Significant	**Low**
Privacy Notice Noncompliance when upgrading the school's CCTV system	Possible	Significant	**Medium**

6. Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
		Eliminated reduced accepted	*Low medium high*	*Yes/no*

CCTV & ingress of water	Use of waterproof enclosures	Reduced	Low	*yes*
CCTV Maintenance	Maintenance contract in place with Security Services	Reduced	Low	*yes*
Training	Undertaken in GDPR and Information Security	Reduced	Low	*yes*
CCTV Passport to Compliance	Upgrade CCTV using guidance from CCTV Passport to Compliance	Reduced	Low	*yes*

Compliance Statement

I can confirm that this data protection impact assessment has been completed to the best of my knowledge and that the technology complies with the data protection principles under GDPR.

All privacy risks and solutions have been considered and represent a proportionate response to the identified risks to personal data.

Signed: Date:

DPO Statement

I can confirm that I have reviewed the DPIA above and are satisfied that the school has taken appropriate steps to protect the data.

DPO Additional advice:

Signed: Date: