CCTV Policy

Code: NS29

Date of approval: 24th March 2021

Date of next review: Spring 2025

Agreed by Whitchurch Primary School Governing Body	Name
Chair of Governing Body	Peter Tenconi
Headteacher	Caroline Rowley

Version	Date	
1	March 21	New Policy
2	March 23	No updates

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 for systems already in existence. (see appendix A)

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:

- To protect pupils, staff and visitors against harm to their person and/or property;
- To increase a sense of personal safety and reduce the fear of crime;
- To protect the school buildings and assets;
- To support the police in preventing and detecting crime;
- To assist in identifying, apprehending and prosecuting offenders;
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence;
- 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 Whitchurch Primary School & Nursery. There are 28 cameras at Whitchurch. The CCTV system used by the school comprises of:

CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL/FIXED
Hyper-Drive DVR	Main school entrance gates - external	No	Yes	Fixed
Hyper-Drive DVR	Marsh lane gates – external	No	Yes	Fixed
Hyper-Drive DVR	Entrance to reception – external	No	Yes	Fixed
Hyper-Drive DVR	Year 2 entrance – external	No	Yes	Fixed
Hyper-Drive DVR	Staff car par – external	No	Yes	Fixed
Hyper-Drive DVR	Outside near the Eco garden - external	No	Yes	Fixed
Hyper-Drive DVR	Upper school computing room – external	No	Yes	Fixed
Hyper-Drive DVR	Upper school playground - external	No	Yes	Fixed
Hyper-Drive DVR	Main reception - Internal	No	Yes	Fixed
Hyper-Drive DVR	Lobby outside the Headteacher's office - Internal	No	Yes	Fixed
Hyper-Drive DVR	All corridors - Internal	No	Yes	Fixed

Statement of Intent

The CCTV system will seek to comply with the requirements both of 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.
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 25 days.

System Management
Access to the CCTV system and data is password protected.
The CCTV system will be administered and managed by Mr. A. Henry, 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 Mr. T. O'Donaghue, the Site Assistant.
The system and the data collected will only be available to the Systems Manager, his replacement and appropriate members of the senior leadership team as determined by the Headteacher.
Where a person other than those mentioned in the paragraph above, requests access to the CCTV data or system, the System Manager will consult with the Headteacher, who will decide the legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.
The CCTV system is designed to be in operation 24 hours a 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 proving 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.
Details of all visits and visitors requesting access, will be recorded on a log sheet, kept safe by the System Manager. Details recorded will be: date, time, person requesting access and details of images viewed and the purpose for so doing. (Appendix B)

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 reference number, date and time;
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.

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

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 Headteacher, Ms. Caroline Rowley.

Public Information
Copies of this policy will be available to the public from the school office.

Appendix A

IMPACT ASSESSMENT – REVIEWING SYSTEMS ALREADY IN PLACE
Name of school: Whitchurch Primary School & Nursery
Assessment carried out by: Katerina Portou & Andrew Henry
Reviewed by DPO On: 3rd March 2021

PURPOSE		
Questions	**Answer**	**Comments**
Does the processing achieve your purpose?	Yes	CCTV is used in and around the School and complies with the Data Protection Act and the most recent Commissioner's Code of Practice.
Is there another, less intrusive, way to achieve the same outcome?	No	N/A
What is your legal reason for processing	See comments	The processing is necessary for the purposes of the legitimate interests pursued by the School or by a third party
RISKS		
Questions	**Answer**	**Comments**
The types of personal data used?	Images of persons in, entering and outside of the School.	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 scale of data used	The CCTV runs 24/7. There are28 cameras in and around the School.	There are 100 members of staff at Whitchurch and 827 children on roll. The school will have regular visitors, outside agencies such as therapists and volunteers
How will data be protected?	Password protected Access only by the Systems Manager and in his absence, the assistant System Assistant	The data is password protected and stored on a hard drive which is in a locked cupboard. Access to the cupboard is by the Site Manager and Site Assistant only.
Will data be shared with third parties	Requests to the Systems Manager and authorised by the Headteacher	Images may be shared with a third party, for example the police for the assistance and prevention of a crime. The System Manager and Headteacher would authorise this and details records would be kept in a log as to who, why and what was viewed.
Potential for harm	Low: procedures are in place for the protection of privacy	The level of harm would be very low if the CCTV policy is followed with robust procedures in place to avoid a data breach as a consequence of illegitimate access to, modification of or loss of personal data resulting in financial loss/breach of privacy/reputational damage/discrimination or loss of confidence.

Data Protection and Security (Risk Mitigation)	
	Comments
Technological security measures put in place by School	The images are password protected and stored in a cupboard which can be accessed only by the Systems Manager and Assistant. This is in a room which is locked at the end of the day. The hard drive is securely stored.
Internal guidance or processes to avoid risks	The Systems Manager and Assistant are aware of the need to avoid risks and will consult with the Headteacher (or Deputy in her absence) on processes including sharing with third parties.
Retention periods for the data	The data will be retained for 25 days.
Levels of access	Only the Systems Manager will have access to the images (and in his absence the Assistant.) The hard drive is secured and in a room which is accessed only by the Manager and Assistant. Any access to a third party (for example the police) will be documented and the log stored.
Other measures	Logs of visitors asking for access to view the images. Any images leaving the School (for example for a criminal investigation) will be authorised by the Headteacher and burned to a disk, sealed, dated, a copy made and stored in the School safe and a detailed log of access kept. There are clear data protection and GDPR notices in the reception area and CCTV signage around the school in line with the transparency principle of GDPR.

School Assessment of Risk		
	Risk Level	Comments
Likelihood of harm to data subject	Unlikely	Level of security is high, policy in place, robust procedures adhered to
Severity of harm (regardless of likelihood)	Minimal	
Overall risk (taking into account measures to reduce risk above)	Low	Likelihood of the risk and the severity of harm remains low
DPO Assessment of Risk		
Likelihood of harm to data subject	Unlikely	
Severity of harm (regardless of likelihood)	Minimal	
Overall risk (taking into account measures to reduce risk above)	Low	

School Compliance Statement
I can confirm that this data protection impact assessment has been completed to the best of my knowledge.

DPO Statement
I can confirm that I have reviewed the DPIA above and am satisfied that the school have taken appropriate and proportionate steps to protect the data OR I confirm that I have reviewed the DPIA above and have made recommendations set out in the comments above which should be accounted for before implementing the above.

Appendix B

CCTV Access Record

Date	**Time**	**Name of person requesting access**	**Reason for request**	**Details of images viewed**	**Authorised by the HT?**	**Name of person granting access**	**Images copied and supplied? Details**