



School Policy Document

CCTV Policy

Date Adopted by Full Governing board: 24 November 2020

Last reviewed on: 26 January 2023

Next review due by: January 2026

Introduction

The school recognises that CCTV systems can be privacy intrusive.

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.

1. Objectives

- 1.1. 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

2. Purpose of this Policy

- 2.1. 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:

Quantity	Camera type
35	Internal Fixed Lens 4MP Dome Camera 4MP High Definition
19	External Fixed Lens 8MP Turret Camera 8MP high resolution
2	Panoramic 20MP 360 Camera 20MP – 4 x 5MP
2	External IR PTZ Dome – 4MP/25 x zoom 4MP resolution

3. Statement of Intent

- 3.1. Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.
- 3.2. 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. Following Brexit, Regulation (EU) 2016/679, General Data Protection Regulation (GDPR) is retained EU law and known as UK GDPR. The UK GDPR sits alongside an amended version of the Data Protection Act 2018 that relate to general personal data processing, powers of the Information Commissioner and sanctions and enforcement. The GDPR as it continues to apply in the EU is known as EU GDPR.
- 3.3. The School will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- 3.4. The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.
- 3.5. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- 3.6. 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.

- 3.7. The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee the system will cover or detect every single incident taking place in the areas of coverage.
- 3.8. 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.
- 3.9. Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.
- 3.10. 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 instructed by the Police or the School's legal representative.

4. System Management

- 4.1. Access to the CCTV system and data shall be restricted.
- 4.2. The CCTV system will be administered and managed by the Headteacher 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 Office Manager.
- 4.3. The system and the data collected will only be available to the Systems Managers, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.
- 4.4. The CCTV system is designed to be in operation for 24 hours each day, every day of the year, though the school does not guarantee that it will be working during these hours.
- 4.5. The System Manager will check and confirm the efficiency of the systems regularly and in particular that the equipment is properly recording and that cameras are functional.
- 4.6. 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.
- 4.7. Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific groups of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.
- 4.8. Where a person other than those mentioned in paragraph 4.2 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.
- 4.9. Details of visitors to the school will be recorded on our electronic entry system including time/date of access.

5. System Management

- 5.1. 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:-
 - Each downloaded media must be identified by a unique mark.
 - Before use, each downloaded media must be cleaned of any previous recording.
 - The System Manager will register the date and time of downloaded media insertion, including its reference.
 - 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.
 - If downloaded media is archived the reference must be noted.

- 5.2. Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement 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.
- 5.3. A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.
- 5.4. 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.
- 5.5. 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.
- 5.6. 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.

6. Complaints About The Use of CCTV

- 6.1. Any complaints in relation to the School's CCTV system should be addressed to the Headteacher

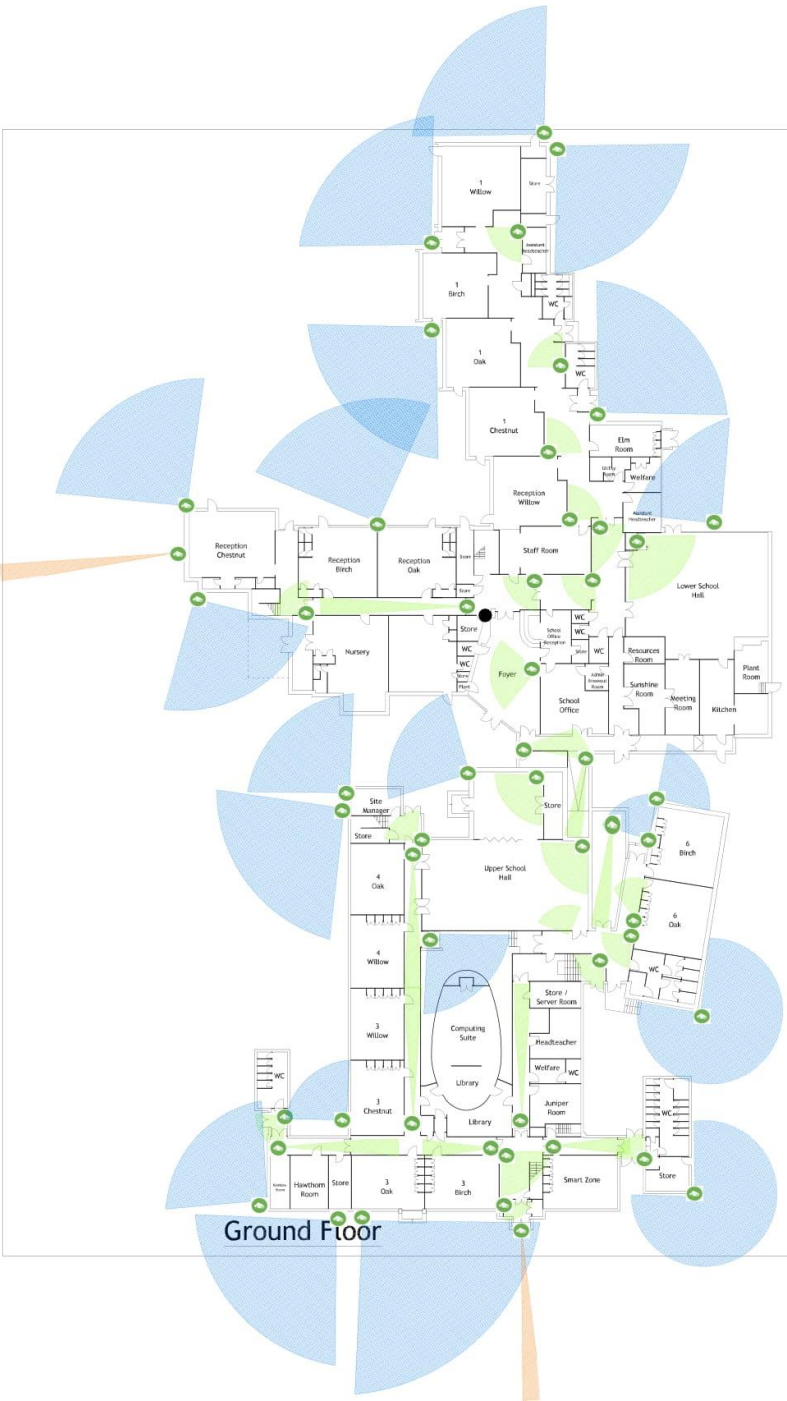
7. Request For Access By the Data Subject

- 7.1. 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.
- 7.2. The Headteacher will consider any request carefully to ensure that access to the images will not breach the security of other people whose images might be contained in the data.
- 7.3. The data may be viewed in one of the following ways:-
 - Directly on the CCTV monitor.
 - On the System Manager's PC (images will be on a secure network in a password protect folder that can only be accessed by authorised personnel).
 - Via a secure/password protected memory stick or pen drive.




8. Public Information

- 8.1. A copy of this policy will be available to the public on our website or copies can be obtained from the school office.

Pinner Park Primary School CCTV Layout



Key

-  Internal, fixed camera
-  External, fixed camera
-  External, adjustable camera