



THE NORTON
KNATCHBULL
SCHOOL

CCTV Policy

Reviewed by	Site Manager
Approved by Finance & General Purposes Committee	22 nd November 2021
Date of Review	January 2023

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.

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 the 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:

Digital NVRS

camera type	Location	swivel/fixed
IP	Gate	fixed
IP	reception entry	fixed
IP	Corridor from S06	fixed
IP	Fraser changing room corridor (inside)	fixed
IP	Fraser Entry door (inside)	fixed
IP	Fraser 6th form common room	fixed
IP	Library Door	fixed
IP	Student reception from Library	fixed
camera type	Location	swivel/fixed
IP	Brabourne fire exit next to B04	fixed
IP	Brabourne Lift first floor	fixed
IP	Ping pong table area	fixed
IP	Music corridor	fixed
IP	Outside G16	fixed

IP	Canteen Right till	fixed
IP	Canteen left till	fixed
IP	Canteen grab n go	fixed
IP	Main entry doors next to the hall (inside)	fixed
IP	Reception area - view to G20	fixed
IP	Toilets door and fire exit next to M08	fixed
IP	Fire door next to M02	fixed
IP	Toilets door first floor Mortimore next to lift	fixed
IP	Corridor from F08	fixed
IP	Toilets door second floor Mortimore next to lift	fixed

OLD NVRS

camera type	Location	swivel/fixed
Analog	Woodwork EXIT	fixed
Analog	Woodwork Gate	fixed
Analog	M08 Fire Exit	fixed
Analog	Front Car park entrance	fixed
Analog	Exit Lane	fixed
Analog	From of the school (tree)	fixed
Analog	Right Entrance	fixed
Analog	The courtyard next to the hall	fixed
Analog	Left entrance	fixed
Analog	Rotating Car park	swivel/fixed
Analog	basketball court	fixed
Analog	basketball court benches	fixed
Analog	G03 Gate	fixed
camera type	Location	swivel/fixed
Analog	Back of D03	fixed
Analog	Kitchen Gate	fixed
Analog	Brabourne Field-Side 1	fixed
Analog	Brabourne Field-Side 2	fixed
Analog	Gate to joey's Lane	fixed
Analog	Repro courtyard	fixed
Analog	Brabourne to Gym	fixed
camera type	Location	swivel/fixed
Analog	Fraser Stairs Drama	fixed
Analog	Fraser Outside R01	fixed
Analog	Fraser Left entrance	fixed
Analog	Fraser Right entrance	fixed
Analog	Fraser Hall Far-right	fixed
Analog	Fraser Hall Front Left	fixed

Analog	Fraser Gym	fixed
Analog	Fraser Common room next to the door.	fixed
Analog	Fraser towards staircase and tennis courts	Swivel

Statement of Intent

A 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 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 have 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 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 one month.

System Management

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

The CCTV system will be administered and managed by the Network Manager, who will take responsibility for restricting access, by the principles and objectives expressed in this

policy. In the absence of the Systems Manager, the system will be managed by the Assistant Network Manager.

The system and the data collected will only be available to the Systems Manager, the Assistant Network Manager, the Site Manager, and the Designated Safeguarding Lead who is a member of the Senior Leadership Team.

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

Cameras have been selected and positioned 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 by the Regulation of Investigatory Power Act 2000.

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

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

Downloading Captured Data onto other Media

To maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any download media used to record events from the hard drive must be prepared by the following procedures: -

- (a) Each download media must be identified by a unique mark.
- (b) Before use, each download media must be cleaned of any previous recording.
- (c) The System Manager will register the date and time of download media insertion, including its reference.
- (d) Download 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 download 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 download 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 Network Manager, the Assistant Network Manager, the Site Manager, the Designated Safeguarding Lead, and the Head Teacher. However, where one of these people may be later called as a witness to an offense 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 of the viewing or release of any download 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 download media (and any images contained thereon) remains the property of the school and download media (and any images contained thereon) are to be treated by 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 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 the Head Teacher in consultation with the School's Data Protection Officer.

Complaints about the use of CCTV

Any complaints about the school's CCTV system should be addressed to the Head Teacher.

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 data held about themselves, including those obtained by CCTV. Requests for such data should be made to the Head Teacher.

Public Information

Copies of this policy will be available on the School website