



Things done well make the best memories

SIR NORTON KNATCHBULL – 1637

CCTV Policy

Policy Owner	Site Manager
Reviewed by	Pat Aird, Site Manager Kevin Robin, Network Manager & Lena Seed, Data Lead
Equality Impact Assessment*	Pat Aird,
Delegated authority	Finance & General Purposes Committee
Approved by the Finance & General Purposes Committee	3 rd October 2026
Date of Review	October 2027
Publication	School website

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 conducted bi-annually and whenever new equipment is introduced, a review will be conducted and a risk assessment put in place.

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.

Lawful Basis

The School's Lawful basis for processing CCTV is **UK GDPR Article 6(1)(e) – Public Task** (for general security and safeguarding) and **Article 9(2)(g) – Substantial Public Interest** (where monitoring relates to safeguarding concerns)

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.

CCTV cameras are in areas where individuals would have an expectation of privacy. These are in the washrooms. We have carried out a Data Protection Impact Assessment (DPIA) to assess the risks and have engaged in stakeholder communication with parents/carers and staff prior to installing them in these areas.

Statement of Intent

The CCTV system will seek to comply with the requirements both UK General Data Protection Regulation (UK GDPR) and the most recent Commissioner's Code of Practice. The school will review its ICO registration annually and conduct a Data Protection Impact Assessment (DPIA) before installing new CCTV units to assess privacy risks.

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.

CCTV Camera Locations

The CCTV system used by the school comprises of:

Ubiquiti NVR

Manufacturer	Location	Swivel/Fixed
Ubiquiti	Brabourne - first floor boys Toilet	Fixed
HikVision	Car Park - Bins	Fixed
HikVision	Car Park – DLC Car Park	Fixed
HikVision	Car Park – Exit Gate	Fixed
HikVision	Car Park – Facing Exit Gate	Fixed
HikVision	Car Park - Front gate	Fixed
HikVision	Car Park – Willow tree	Fixed
HikVision	DLC – Entrance Lobby	Fixed
HikVision	DLC - First Floor Circulation	Fixed
HikVision	DLC – First Floor Lobby	Fixed
HikVision	DLC – Ground Floor Circulation	Fixed
HikVision	DLC – Ground Floor Fire Exit	Fixed
HikVision	DLC – Outside Front Door	Fixed
HikVision	DLC – Outside Front Door 2	Fixed
HikVision	DLC – Outside Left Hand Side	Fixed
HikVision	DLC – Outside Rear	Fixed
HikVision	DLC – Outside Right Hand Side	Fixed
Ubiquiti	Fraser - ground floor boys Toilet	Fixed
HikVision	Fraser – Left Entrance R01	Fixed
HikVision	Fraser – Middle Entrance R05	Fixed
HikVision	Fraser – R02 Common Room	Fixed
HikVision	Fraser – R15	Fixed
HikVision	Fraser – R19 to R11 Drama	Fixed
HikVision	Fraser - Right entrance CR-C	Fixed
Ubiquiti	Mortimore - First Floor Sinks	Fixed
HikVision	Mortimer - First Floor Toilets	Fixed

HikVision	Mortimer - Ground Floor Toilet	<u>Fixed</u>
Ubiquiti	<u>Mortimore - Second floor Sinks</u>	<u>Fixed</u>
HikVision	Mortimer - Second Floor Toilet	<u>Fixed</u>
Ubiquiti	<u>Music Toilets - Sinks</u>	<u>Fixed</u>
HikVision	<u>Outside - G15 From Gate</u>	<u>Fixed</u>
HikVision	<u>Outside - Quadrangle</u>	<u>Fixed</u>

Note:

Ubiquiti cameras have audio capability but it is switched off on recording and controlled by the Network Manager and Site Manager.

The HikVision Cameras are connected to the Ubiquiti NVR through ONVIF (secured by a Username / password).

Hikvision NVR 3

Manufacturer	Location	Swivel/Fixed
HikVision	Mortimer - 2FL - Stairs	swivel/fixed
HikVision	Mortimer - 1FL - Stairs	fixed
HikVision	S06 to S04	fixed
HikVision	Reception - Main Entrance	fixed
HikVision	Library Main Desk and PCs	fixed
HikVision	M26 To M23 and M21	fixed
HikVision	G03 Toilets	fixed
HikVision	Art Courtyard	fixed
HikVision	B26 To B32	fixed
HikVision	B01 to Entrance	fixed
HikVision	G04 - Toilets	fixed
HikVision	G20	fixed
HikVision	Outside - Astro and Field	fixed
HikVision	Outside - Basketball Court	fixed

Hikvision NVR 5

camera type	Location	swivel/fixed
HikVision	Hall	fixed

HikVision	Brabourne - FF - Toilets	fixed
HikVision	Outside - Ping Pong Area	fixed
HikVision	Music Office Corridor	fixed
HikVision	G16 to Hall	fixed
HikVision	Canteen - Right	fixed
HikVision	Canteen - Left	fixed
HikVision	Canteen - Sixth Form Till	fixed
HikVision	Entrance - Left from Inside	fixed
HikVision	Reception and G20 entrance	fixed
HikVision	Mortimer - Fire Exit near M03	fixed
HikVision	Brabourne - F08 Corridor	fixed
HikVision	Brabourne - B04 to B08	fixed
HikVision	Brabourne - Fire Exit near B08	fixed

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. App access (through Ubiquiti Protect) will be restricted to the Site Manager (for late night emergency monitoring), Network Manager and Assistant Network Manager (both Admins).

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 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 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 Headteacher in consultation with the School's Data Protection Officer.

Complaints about the use of CCTV

Complaints

Staff complaints and enquiries about how the operation of our CCTV system affects their conditions of employment should be made in line with the School's Grievance Procedure available on the staff portal. For all other complaints or queries about how the system affects individuals' data protection rights, staff, parents, students, and visitors will find information about our Data Protection Complaints Procedure available on the school website.

If a member of staff believes that there has been a breach of the Data Protection Act, or any other legal obligations, they should contact the data lead as a matter of urgency in accordance with the data breach reporting process set out in our Data Breach Policy.

Request for Access by the Data Subject

UK GDPR 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. Such requests can be made under Subject Access Request to gdpr@nks.kent.sch.uk.

NKS – Equality Impact Assessment

The purpose of an Equality Impact Assessment (EIA) is to ensure that policies, functions, plans or decisions do not create unnecessary barriers for people protected under the Equality Act 2010. Where negative impacts are identified these should be eliminated or minimised, and opportunities for positive impact should be maximised.

POLICY STATUS	
Update of existing policy	
THIS POLICY WILL AFFECT	
Staff Students Teachers Parents Visitors to the school site General public passing by school gate	
EIA completed by:	Lena Seed, Data Lead
Contributors to EIA:	Pat Aird, Site Manager
Date completed:	21 st February 2025 and revised 14 th March 2026

Impact analysis

GROUP	POSITIVE IMPACT	NEUTRAL IMPACT	NEGATIVE IMPACT	WHY WILL THE POLICY HAVE THIS EFFECT?
Sex		ü		Policy applies equally to all genders.
Race		ü		No racial profiling; CCTV use is universal.
Religion or belief		ü		No interference with religious practices.
Sexual orientation		ü		No impact on this characteristic.
Gender reassignment		ü		Policy applies equally to all identities.
Pregnancy or maternity	ü			CCTV may assist in responding to accidents, medical incidents or safeguarding concerns affecting pregnant staff, students or visitors and contributes to maintaining a safe environment.
Age		ü		Protects all age groups equally.

Disability /SEND		ü		CCTV may provide additional reassurance and protection for disabled pupils, staff and visitors. The school will ensure that the operation of CCTV remains proportionate and that any associated processes remain accessible and responsive to disability-related needs.
Marriage or civil partnership		ü		No direct impact.
Any non-protected characteristics that have a specific impact in your school, e.g.: - English as an additional language - Looked-after children - Families with separated parents		ü		no impact on non-protected characteristics have been identified

INTERSECTIONAL IMPACT

No adverse intersectional impacts have been identified. CCTV monitoring is determined by safeguarding, security and operational requirements rather than personal characteristics, and applies consistently across all protected groups.

Outcomes

The EIA has identified no adverse equality impacts arising from the policy. CCTV is used to support safeguarding, safety, security and the prevention and investigation of incidents. The school has undertaken a DPIA in relation to CCTV coverage, including cameras located within identified washroom areas, and will continue to monitor implementation to ensure that privacy, dignity and equality considerations remain appropriately balanced with safeguarding requirements. The assessment will be reviewed whenever equipment, coverage or operational arrangements change.

CONSULTATION AND STAKEHOLDER ENGAGEMENT

Parental communication regarding the introduction of the CCTV in washrooms took place in T5 2026. No concerns from parents were received.

