St Paul's School

FOUNDED 1509

CCTV Policy

Author/reviewer responsible:	Operations and Compliance Manager	Date of last review:	06/25
Reviewed by:	E-Safety Committee	Date of authorisation:	08/25
Authorised by resolution of:	Full Governing Body	Date of next review:	06/26
Applicable:	SPJ & SPS		

This policy is available on the Handbook page of the School Intranet and policies page of the School website and can be made available in large print or other accessible format if required; such requests can be made to policyquery@stpaulsSchool.org.uk

CCTV Policy

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.

Objectives

Review of this policy shall be repeated regularly and, whenever new equipment is introduced, a review will be conducted and a data protection impact assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist the School in reaching the following 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 and other law enforcement authorities 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 monitor and uphold discipline among pupils in line with the Behaviour, Rewards and Sanctions Policies, which are available on the School website; and

(h) 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 Type	Internal/ External	Location	Sound	Recording Capacity	Swivel/ Fixed
HikVision	External x1	SPJ Junior Reception	N	Y	F
	Internal x1	SPJ Junior Reception	N	Y	F
	External x3	SPJ Big Side	N	Y	F
	External x2	Centenary Building	N	Y	F
	Internal x5	Performance Health Centre	N	Y	F
	External x1 (ANPR)	Entrance Road	N	Y	F
	External x8	Boat House	N	Y	F
	External x1	Main Carpark	N	Y	F
	External x2	Bowl Carpark	N	Y	F
	External x2	East Pavilion	N	Y	F
	External x1	West Pavilion	N	Y	F
	External x3	Wathen Hall	N	Y	F
	External x2	East House	N	Y	F
	External x5	SPJ Pavilion	N	Y	F

	External x3	Hammersmith Gate	N	Y	F
	External x1	Main Entrance	N	Y	F
	External x 2	ANPR on Main Entrance Barrier	N	Y	F
BMS	External x10	Entrance Roads, Main/Small Carpark, Parking Bays, Statue	N	Y	F
	Internal x1	Security Hut	N	Y	F
	External x8	West Pavilion, West House, SPJ Pavilion	N	Y	F
	Internal x2	SPJ Pavilion	N	Y	F
	External x6	SPJ Music, Centenary Building	N	Y	F
	External 11	Colet House, School House, Wathen Hall, Service Rd, Boat House, Dorfman Theatre	N	Y	F
	Internal x4	Dorfman Theatre	N	Y	F
	External x7	Big Side, Hammersmith Gate, St. Hilda's, East Pavilion	N	Y	F
	External x4	Engineering, Ichthys, Bike Sheds	N	Y	F
	External x2	Sports Block	N	Y	F
	Internal x4	Sports Block	N	Y	F
	External x10	GTB 1&2, Atrium, Founder's Court, Reception, Science Building, IT	N	Y	F
	Internal x56	GTB 1&2, Atrium, Founder's Court, Reception, Science Building, IT, Lockers	N	Y	F

Locations have been selected, both external and internal, which the School reasonably believes require monitoring to address the stated objectives. CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

The CCTV system will seek to comply with the requirements of the Data Protection Act, the UK GDPR, the most recent Commissioner's Code of Practice and the National Minimum Standards for Boarding relating to biometrics and surveillance.

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 School has endeavoured, in the planning and design of the system, to ensure that it will give maximum effectiveness and efficiency, however 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.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of 21 days.

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 a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than is necessary. The ongoing need to retain this data will be reviewed at least every six months.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by The Security 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 Security Supervisor, the Head Porter or the Facilities Manager.

The system and the data collected will only be available to the Systems Manager, nominated members of the security team, their replacement and appropriate members of the senior leadership team as determined by the High Master, the Surmaster, the Head of St Paul's Juniors or the Director of Operations.

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 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.

Where a person other than those mentioned above, requests access to the CCTV data or system, the System Manager must satisfy themself of the identity and legitimacy of 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 log book including time/date of access and details of images viewed and the purpose for so doing.

Downloading Captured Data on to 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 dated and stored by the System Manager in a separate secure evidence store and recorded in the system log. If a downloaded media is not uploaded to the secure police portal before it is stored, an upload may be made at a later date by the System Manager; this must be dated and recorded in the system log.

(e) If downloaded media is archived, the reference must be noted.

(f) If downloaded media is put onto a device, the device will be encrypted and password protected.

Images may be viewed by the police for the prevention and detection of crime, insurance companies when submitting a formal request and by the Systems Manager, his/her replacement and the High Master 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 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 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 a senior leader of the School in consultation with the School's Data Protection Officer.

Other CCTV systems

The School does not own or manage third party CCTV systems, but may be provided by third parties with images of incidents where this in line with the objectives of the School's own CCTV policy and/or its School Rules.

Many pupils travel to School on buses or coaches provided by third party contractors and a number of these coaches are equipped with CCTV systems. The School may use these in establishing facts in cases of unacceptable pupil behaviour, in which case the parents/guardian will be informed as part of the School's management of a particular incident.

Complaints About the Use of CCTV

Any complaints in relation to the School's CCTV system should be addressed to The Director of Operations.

Requests 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 DPO@stpaulsschool.org.uk .