



ROSEMEAD
PREPARATORY
SCHOOL & NURSERY
DULWICH

P14.2 – CCTV Policy

Preparatory Department

70 Thurlow Park Road, Dulwich

London SE21 8HZ

Tel: 020 8670 5865

Pre-Preparatory & Nursery

40A Thurlow Park Road, Dulwich

London SE21 8HZ

Tel: 020 8761 1307

www.rosemeadprep.org.uk

Introduction

Rosemead Prep School & Nursery (the School) recognises 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 risk 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:

- 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 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; and
- 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	Location	Sound	Recording Capacity	Swivel/Fixed
Bullet Camera	Main Prep entrance	N	N	F

Bullet Camera	Main Pre-Prep facing the stepped entrance	N	N	F
Bullet Camera	Main Pre-Prep facing the sloped entrance	N	N	F
Bullet Camera	Prep playground facing the sloped entrance	N	N	F
Bullet Camera	Prep playground facing the kitchen entrance	N	N	F
Bullet Camera	Pre-Prep Playground	N	N	F
Bullet Camera	Nursery Playground	N	N	F

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 predominantly 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 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 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 30 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 6 months.

Roles and responsibilities

The governing body

The governing body has the ultimate responsibility for ensuring that the CCTV system is operated within the parameters of this policy.

The Chief Operating Officer

The COO will:

- Take responsibility for effective management of the CCTV system.
- Liaise with the Data Protection Officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated objectives and that its use is needed and justified.
- Review the CCTV policy regularly to check that the Foundation remains compliant with legislation.
- Ensure that all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and data protection.
- Sign off any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of the data protection impact assessment.

- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

The Head of Operations

The Head of Operations will:

- Ensure that the guidance set out in this policy is followed by all staff.
- Train persons with authorisation to access the CCTV system on the data protection implications (storage, sharing footage, access).
- Consider and approve internal requests to review footage.
- Train all staff to recognise a Subject Access Request.
- Deal with Subject Access Requests which are handled under the Data Protection Act 2018.
- Ensure footage is retained in a legal, fair and transparent manner.
- Ensure footage is destroyed when it falls out of the retention period.
- Keep accurate records of all data processing activities and make the records public on request.

The Data Protection Officer

The DPO will:

- Monitor compliance with UK data protection law.
- Advise on and assist the Foundation with carrying out data protection impact assessments.
- Act as a point of contact for contact for communications from the Information Commissioner's Office.
- Conduct data protection impact assessments.
- Ensure data is handled in accordance with data protection legislation.
- Inform subjects of how footage of them will be used by the Foundation, what their rights are, and how the Foundation will endeavour to protect their personal information.
- Ensure that the CCTV system is not infringing on an individual's reasonable right to privacy in public spaces.
- Receive and consider requests for third-party access to CCTV footage.

The System Manager

The System Manager, who is the IT Manager, will:

- Be responsible for the day-to-day management, maintenance and operation of the CCTV system.
- Oversee the security of the CCTV system and footage.
- Check the system for faults and security flaws termly.
- Check that data and time stamps are accurate termly.
- Ensure that CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified.
- Carry out termly checks to determine whether footage is being stored accurately and being deleted after the retention period.

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 IT Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy.

The system and the data collected will only be available to the Systems Manager, the Head of Operations, the COO, the Head and appropriate members of the senior leadership team as determined by the Head.

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 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 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 him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused and referred to the COO and Headteacher.

Details of all visits and visitors will be recorded in a system log book including time/data 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: -

- 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.
- 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 and by the Systems Manager, the Head of Operations, the COO, the Head 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.

Complaints About the Use of CCTV

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

Public Information

Copies of this policy will be available to the public from the School office.