

SHANGHAI AMERICAN SCHOOL

CCTV Policy

Introduction

The CCTV system is installed on our campuses to meet regulatory requirements and to promote the safety and security of our community. We understand that individuals may have concerns about how the CCTV system affects their privacy. This policy is designed to address typical privacy concerns and to detail the proactive measures the school has put in place to ensure responsible surveillance.

Images recorded by the CCTV cameras are personal information which must be processed in accordance with data protection laws. We are committed to complying with our legal obligations and ensuring the privacy rights of staff, students and visitors are recognized and respected.

This Policy will therefore outline why we use camera surveillance, how we use it and how we process the information we capture to ensure we are compliant with data protection laws and best practices.

This policy applies to all staff, contractors, students and visitors at Shanghai American School.

Responsible Personnel

The Data Protection Lead is responsible for the overall management of this Policy and for ensuring compliance with the relevant legislation. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it will be disclosed has been delegated to the Security Office. Operational responsibility for the cameras and the storage of data is the responsibility of the Security Office.

Reasons for the use of CCTV

We currently use CCTV throughout our school for the following purposes:

- for the security and personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime;
- to detect and delay crime and to protect buildings and assets from damage, disruption, vandalism and other crime;
- to enable prompt and effective responses to incidents;
- to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;
- to assist in the defense of any civil litigation, including employment proceedings;
- to support law enforcement bodies in the prevention, detection and prosecution of crime;

- to assist in day-to-day management, ensuring the health and safety of staff, students, visitors and other members of the public.

This list is not exhaustive and other purposes may be or become relevant.

We consider the use of CCTV to be in our legitimate interests to protect property and to maintain the safety of individuals.

Location of Cameras

Camera locations comply with the regulations set by the Shanghai Municipal Education Commission and national standards. The location of each camera is carefully chosen so that it will only monitor the area relevant to the intended purpose and to ensure that it is not positioned in an area where there is an expectation of privacy (e.g. changing rooms and toilets).

CCTV cameras are located in areas defined in the national standards (*Safety prevention requirements for primary and secondary schools and kindergartens*), including

- Outside the school gate;
- School perimeter;
- School entrances and exits;
- Security Central room;
- Outdoor areas for concentrated activities;
- Playgrounds;
- Building main entrances and exits;
- Canteen operation area and dining area;
- Storage rooms and laboratories for hazardous materials;
- Storage areas for valuable items;
- Vehicle parking areas

System Operations

Our cameras are not used to record sound but are in operation 24 hours a day, 365 days a year.

We ensure that signs are displayed at entry points to the school to alert individuals that their images may be recorded.

Images collected by CCTV are viewed in secure offices by authorized members of staff whose role requires them to have access to the data. This may include HR staff involved with disciplinary or grievance matters.

Live video feeds are monitored only in the security control room to detect abnormalities and respond accordingly. This room is equipped with additional surveillance cameras, and access is restricted to authorized personnel only.

Storage of Data

In order to ensure that the rights of individuals recorded by the CCTV system are protected, we ensure that data gathered from CCTV cameras is stored in a way that maintains its integrity and security. This may include encrypting the data, where it is possible to do so.

We may engage data processors to process data on our behalf. We ensure the necessary contractual safeguards are in place to protect the security and integrity of the data.

Data Retention

Images are required to be stored for a minimum of 90 days and will be automatically deleted following the system limitations unless the images are required as evidence or for a purpose stated above.

Once the purpose for holding the images has been fulfilled, all images will be erased permanently and securely. Any physical matter, such as still photographs, hard copy prints, tapes or discs, will be disposed of as confidential waste.

Management of CCTV

Before the introduction of any new CCTV cameras, we carefully consider where they are placed and what data they will capture by carrying out a Personal Information Protection Impact Assessment (PIPIA). This process is intended to assist us in deciding whether the new cameras are necessary and proportionate to the circumstances.

Review of CCTV use

We ensure that the use of our existing CCTV cameras is reviewed periodically, and at least on an annual basis, to ensure that the images are clear and high quality. We also ensure that their use remains necessary and appropriate and that we are continuing to address the needs that justified the cameras' initial introduction.

Requests for Disclosure

We may allow appropriate law enforcement agencies to view or remove CCTV footage where this is required for the detection or prosecution of a crime.

We may also release CCTV footage to a third party where it is required for legal proceedings or has been requested by way of a court order.

We maintain a record of all disclosures of CCTV footage.

We do not post images captured on CCTV online or disclose them to the media.

Subject Access Requests (SARs)

Individuals may make a request for the disclosure of their personal data and this may include CCTV images. This is called a Subject Access Request. Information about how to exercise this and other rights can be found in the Subject Access Rights Policy.

To enable us to locate relevant footage, any requests for recorded CCTV must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual concerned.

We reserve the right to obscure images of third parties when disclosing CCTV images as part of a subject access request, in all cases where we consider it necessary to do so.

Contact Us

The Data Protection Lead is responsible for overseeing this Policy. Our Data Protection Lead can be reached at dataprotection@saschina.org.