

Guidelines for Use of Security Cameras

Guidelines for Use of Security Cameras

Introduction	1
Scope	1
Responsible Personnel	1
Reasons for the Use of Security Cameras	1
Location of Cameras	2
System Operations	2
Access to and Use of Recorded Footage	2
Reviewing of Security Camera Footage	2
Storage of Data	3
Data Retention	3
Management of Security Cameras	3
Review of Security Camera Use	3
Requests for Disclosure	3
Contact us	3

Introduction

We currently use security cameras on school premises in order to help us maintain a safe and secure environment and we recognise that individuals may have privacy concerns about such filming. These guidelines are intended to address those concerns and to provide reassurance about the safeguards we have in place.

Images recorded by the security cameras are considered personal data 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 recognised and respected.

These guidelines will therefore outline why we use camera surveillance, how we use it and how we process the data we capture to ensure we are compliant with data protection law and best practice.

Scope

These guidelines apply to all video footage taken by school-owned security cameras on school grounds and access to such footage by designated members of staff.

Responsible Personnel

The Data Privacy Officer is responsible for the overall operation of security camera systems and for ensuring compliance with these guidelines and 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 Data Privacy Officer. Operational responsibility for the cameras and the storage of data is the responsibility of the Data Privacy Officer.

Reasons for the Use of Security Cameras

We currently use security cameras on school premises for the following purposes:

- To support the security and personal safety of staff, students, visitors and other members of the public and to act as a deterrent against crime;
- To prevent and detect crime, including protection of buildings and assets from damage, disruption, vandalism and other crime;

- To assist in the effective resolution of disputes which may arise in the course of disciplinary or grievance proceedings;
- To assist in the defence 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 security cameras to be in our legitimate interests to protect property and to maintain the safety of individuals.

Location of Cameras

The location of each camera is carefully chosen so that it will only monitor the area relevant for 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).

Security cameras are located around campus and building entrances and perimeters, as well as some common outdoor areas, such as the playground, and some interior spaces, including the swimming pool.

System Operations

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

Access to and Use of Recorded Footage

Review of recorded security camera footage will occur only by authorized personnel and when there is a reported claim of an injury or an incident that raises safety or security concerns. A note stating that stored footage was reviewed, and by whom, should be added to the incident report or other documentation.

Reviewing of Security Camera Footage

Permissions to access security camera system

For the protection of privacy, access to the security camera system is only available to members of the Senior Leadership Team (SLT), Director of IT, IT Operations Manager, Safeguarding Lead and the Facilities and Legal Affairs Manager. To support investigating an incident, other members of staff may view security camera footage upon request by a member of the Senior Leadership Team and with the SLT member present.

Logging of access

The security camera system logs all video viewing sessions. The information logged includes which camera was accessed, the user that accesses the camera footage and the date/time the video was viewed. Logs are stored for one year before being deleted automatically.

Timely access to footage

Once an incident is reported security camera footage should be reviewed within 2 working days.

Downloading and/or archiving of footage

Video footage will be automatically deleted by the security camera system after 30 days. If an incident requires a longer retention period, the footage must be exported from the security camera system, downloaded and uploaded to the Security Shared Drive. Only users with security camera system access can export footage and must ensure that data is permanently deleted from their computer after it has been uploaded to the Security Shared Drive.

Reviewing footage of safeguarding incidents

If a safeguarding incident, as defined in the YIS Safeguarding: Student Protection Policy and Guidelines, requires the viewing of security camera footage, it must be reviewed by one member of the Senior Leadership Team AND another member of the Senior Leadership Team OR the Safeguarding Lead.

Storage of Data

In order to ensure that the rights of individuals recorded by the security cameras system are protected, we ensure that data gathered from security 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 store images recorded by the security cameras locally or using a cloud computing system. We take reasonable steps to ensure that any cloud service provider maintains the security of this information. 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 will be automatically deleted after 30 days unless the images are required as evidence or for a purpose stated above which requires a longer retention period, in which case the images will be deleted once that purpose has been fulfilled. 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 Security Cameras

Prior to the introduction of any new security cameras, we carefully consider where they are placed and what data they will capture. This process is intended to assist us in deciding whether the new cameras are necessary and proportionate in the circumstances.

Review of Security Camera Use

We review the use of our existing security cameras periodically to ensure that their use remains necessary and appropriate.

Requests for Disclosure

Live or recorded security camera footage may only be disclosed externally with the written permission of the Head of School. We may allow appropriate law enforcement agencies to view or remove security camera footage where this is required for the detecting or prosecution of crime. We may also release security 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 security camera footage. Under no circumstance will we post images captured on security cameras online or disclose them to the media.

Parent/Student Access

With the exception of law enforcement authorities, if they so request, persons other than those designated by the Head of School or other member of the Senior Leadership Team to investigate an incident may not have direct access to security camera footage. Specifically, in discussing an incident with parents or students who are directly involved or implicated in the incident, the Head of School or Senior Leadership Team member is under no obligation to share security camera footage with the relevant student and/or parent, but may do so at their discretion.

Contact us

If you have any questions or concerns relating to this policy please contact our Data Protection Officer at dpo@yis.ac.jp.