HARROW
HONG KONG CHILDREN SCHOOL
哈罗港人子弟学校
SHENZHEN QIANHAI 深圳前海

Closed Circuit Television (CCTV) Policy for Parents (HHKCS-2.2.8)

Last updated (by): 29 January 2024 (NSC)

1. INTRODUCTION

In the effort to create and maintain a safe and secure environment for students and staff, CCTV systems are employed to assist School leadership in detecting and deterring unacceptable behaviour or activities, to deter against and aid in the identification of intruders, and to provide a historical record to assist in investigation.

1.1 SCOPE

This policy applies to all types of camera surveillance systems, surveillance monitors and camera recording devices that are used for security purposes at any School-owned and leased properties.

1.2 RATIONALE

The intent is to ensure that, in adopting the use of video surveillance cameras, the School balances the security, safety and other benefits derived from the use of video surveillance with the privacy rights of the individual.

1.3 BASIS

In the daily operation of the School premises, the safety of students, staff, parents, visitors and property is protected and maintained by conventional means such as: alert observation by staff, foot patrols by security personnel, security-conscious design of School campuses, and the consistent application of the School's policies and procedures in relation to Facilities, Health and Safety and Safeguarding. The protection provided by surveillance cameras augments other security means and is an essential component in maintaining lawful and safe use of the School campus.

2. PROCEDURES STATEMENT

The CCTV Procedures provides detailed direction concerning the context, procedures and protocols within which the School installs and operates surveillance cameras.

SYSTEM DESIGN:

2.1 Designing and CCTV Equipment:

2.1.1 Given that School facilities are accessible at all times and the constant possibility of intruders, there is a need to provide video surveillance at all hours of the day and night. The video equipment shall be installed to monitor only those spaces that have been identified as requiring video surveillance, according to para 1.2.1 and 1.2.2 below;

2.1.2 The ability of authorised personnel to adjust cameras shall be restricted so that unauthorised personnel cannot adjust or manipulate cameras to overlook spaces that are not intended to be covered by the video surveillance programme;

2.1.3. Equipment shall never monitor the inside of areas where students, staff, parents and visitors have a higher expectation of privacy (e.g. changing rooms and toilets, nappy changing spaces in EY classrooms, offices);

2.1.4. Recording equipment must be located in a strictly controlled access area, normally the ICT room or a guard room. Only authorised personnel shall have access to the controlled access area. Guards and ICT personnel should not have routine access to any recordings. Instead, access to recordings must only be strictly controlled and accessed by personnel authorised by Approvers (hereafter referred to as Head Master, Deputy Head EYC, Deputy Head Pastoral, and the Head of Operations).

2.1.5 Staff can request access through the Approvers. Authorised personnel should have received school safeguarding and data security training;

2.1.6. Authorised personnel must ensure video monitors are not in a position that enables the public and/or unauthorised staff to view the monitors.

2.2 System Requirements:

2.2.1. Internal coverage of the CCTV system must include: The entrances to all classrooms (including specialist rooms and PE areas), toilets, changing rooms, health clinics, offices, storerooms and maintenance closets, theatres and black boxes. Full coverage of gymnasiums and sports rooms, swimming pools, libraries, stairwells, corridors and back stage areas. Full coverage of Kindergarten classrooms (Toddler-Year 2) and music practice rooms. Full coverage of any office space nominated by the School where private student-staff closed door meetings are deemed permissible. Music rooms and rooms where 1 to 1 practice sessions are undertaken.

2.2.2. External coverage of the CCTV system must include:
• All accessible entrances to the perimeter of the campus (i.e. main gates and side gates);
• General coverage of the campus perimeter;
• General coverage of all playgrounds and play equipment.
• Roads leading from main gates inside the campus

2.2.3 The quality of CCTV imaging should be of a suitable standard, enabling a still to be captured and a person identified under all light conditions. For internal and external cameras, facial recognition should be possible at all times of the day and night, including in low-light and wet conditions.

2.2.4. Access to the CCTV control room must be restricted to listed authorised personnel, with the list held by Head of Operations. It includes the following people: Head Master, Deputy Heads (EYC; Pastoral), Head of Operations Facilities.

2.2.5 To respect the privacy of teachers and ensure a professional working environment, any surveillance equipment directly covering the interior of a classroom or offices must not feed-in to the live television display in the control room. Under no circumstances are recordings to be reviewed for the purpose of assessing teacher performance. Recordings from such cameras are stored in a secure environment and are only accessible by authorised personnel in the event of a reported incident.

2.3 Notice of Use of Video Systems:

2.3.1 The School shall post signs, visible to students, staff, parents and visitors at all entrances and/or displayed on the perimeter of the grounds indicating that the premises is under 24-hour video surveillance.
2.3.2. The notification requirements of this sign must inform individuals that video surveillance is taking place, the purpose(s) for which the personal information is intended to be used and contact information for a person or office who can answer questions about the data collection.

2.4 Personnel Authorised to Operate Video Equipment:

2.4.1. Only authorised personnel shall be permitted to operate video surveillance systems or to edit/delete video records, with proper induction provided. The list of authorised personnel must be approved by the Head of Operations and subject to reauthorisation at the beginning of each academic year, as well as upon relocation of any authorised personnel.

2.4.2. No person shall be authorised to move, black out, or make adjustment to any CCTV surveillance equipment without prior written authorisation from the Head of Operations.

2.4.3. Viewing of CCTV Footage
i. The Approvers shall have the right to access the CCTV control room and view footage at all times.

ii Other staff may view footage on occasions where authorisation is provided by the Approvers via email.
iii All viewing of system data will be in a suitably secure and private area to minimise the likelihood of or opportunity for access by unauthorised persons.
iv Viewing, in this context, will include both real time and retained footage.
v No recording or copying of CCTV footage can be made of any part, or whole, by any personnel without explicit instruction from an authorized approver in writing as per 2.5.4.
vi Parents are not approved under any circumstances to view footage in the CCTV control room.

2.5 Justification for Access to CCTV

2.5.1. The following are examples when the Approvers may authorise access to CCTV images:
i Where required to do so by the Head Master, the Police or some relevant statutory authority;
ii To make a report regarding suspected criminal behaviour;
iii To enable the Designated Safeguarding Lead or his/her appointed deputy to examine behaviour which may give rise to any reasonable safeguarding concern;
iv To assist the School in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardian may be informed as part of the School's management of a particular incident;
v To the School's insurance company where required in order to pursue a claim for damage done to insured property; or
vi In any other circumstances required under law or regulation, or the Approvers' judgements based on the best interests of the School.

2.5.3. A CCTV Log will be maintained to record all access requests, retained footage and viewings. This shall be reviewed monthly by the Head of Operations.

2.5.4 Copying or recording image and footage
i. In the case of Police requests, copies can be made and shared directly with the police authority only, by an authorized person in writing from an approver, and never shared with any other parties or parents.
ii Authorised personnel may record an image, or part of footage, as part of an investigation into behaviours to establish identity, for insurance purposes, or maintain secure records for serious offenses.
iii Where copies of footage, or images, have been made these should be transferred to a secure school owned password protected digital storage, and for serious offenses placed in the DH or HM safe. Under no circumstances should any footage remain on any personal devices.
iv Footage from behaviour investigations will be kept for one year following conclusion of the investigation, after which the record must be destroyed or deleted.
v Footage from severe incidents at level 4 of the behaviour policy will be kept for up to 3 years, after which the record must be destroyed or deleted.

3. VIDEO EQUIPMENT/RECORDS:

3.1 Most camera types including, but not limited to, bullet cameras, dome cameras, Network/IP, infrared and varifocal are acceptable for use provided they are compatible with a network video recording system (NVR) or a digital video recording system (DVR). Where existing cameras are in use and connected to a videocassette recorder (VCR) this is acceptable provided that upon replacement it is upgraded to an NVR or DVR system. Use of motion School CCTV Surveillance Policy recording is permissible and encouraged in certain areas as a way to minimise data storage requirements.

3.2 All records (storage devices) shall be clearly identified (labelled) as to the date and location of origin including being labeled with a unique, sequential number or other verifiable symbol. In facilities with an NVR/DVR that stores information directly on a hard drive, the computer time and date stamp shall be understood to be this identification. In facilities with a VCR or other recording mechanism using a removable/portable storage device, the authorised personnel shall affix a label to each storage device identifying this information.

3.3 The School is required to retain at all times the previous 90 days of recorded data. It is not required that all data be physically stored on School servers if alternative secure storage arrangements are available (e.g. external

storage, cloud storage, software solutions, etc.) and can be suitably safeguarded against hacking. Currently all data is stored on the School servers. All servers and storage media must be kept under lock and key and accessible only by authorised ICT personnel.

3.4 The School retains custody and control of all original video records not provided to law enforcement. With the exception of records retained for criminal, safety, or security investigations or evidentiary purposes, the School will not maintain a copy of recordings for longer than the recording systems' 90 days recording cycle unless specifically requested by the Head Master. The school will take all reasonable efforts to ensure the security of records in its control/custody and ensure their safe and secure disposal. Old storage devices must be disposed of in accordance with an applicable technology asset disposal process ensuring personal information is erased prior to disposal and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

3.5 Each School Campus shall maintain a confidential record of all activities related to video devices and records. Activities include all information regarding the use, maintenance, and storage of records and all instances of access to, and use of, recorded material, including the name of the person accessing the system. All log entries will detail staff name, date, time and activity. Any unusual or suspicious activities must be reported immediately to the Head Master. This record must remain in a lockable safe and secure location with the video recording equipment and must be audited by the Deputy Head (Pastoral) once a term (it is the responsibility of the Head of Operations to ensure that the Deputy Head (Pastoral) reviews the logbook monthly during the academic year). Only authorised personnel may remove this logbook from the secure location.

4. ACCESS TO CCTV ARCHIVE

4.1 Access to the video surveillance records, e.g. logbook entries, DVR, cassettes or CDs, etc. shall be restricted to Authorised personnel, and only in School CCTV Surveillance Policy order to comply with their roles and responsibilities as outlined in the Video Surveillance Policy.

4.2 All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area.

4.3 With the exception of requests by law enforcement agencies or the court, all formal requests for video records should be made in writing and directed to the Head Master.

5. ACCOUNTABILITY

5.1 The Head:

5.1.1 Is responsible and accountable for documenting, implementing, enforcing, monitoring and updating the privacy and access practice of the School;

5.1.2 Informing appropriate shared facilities' personnel of this Policy's requirements if in a shared facility. (e.g. Kindergarten)

5.2 Deputy Head (Pastoral) / Head of Operations:

5.2.1 Is responsible for recommending proposed installations for campus;

5.2.2 Ensuring that all School members of staff are familiar with this Policy and providing advice, training and recommendations to staff;

5.2.3 Overseeing the day-to-day operation of video surveillance cameras, providing supervision to approved authorised personnel, and ensuring their compliance with all aspects of this Policy;

5.2.4 Ensuring monitoring and recording devices, and all items related to surveillance (e.g. logbooks) are stored in a safe and secure location;

5.2.5 Ensuring logbooks recording all activities related to security video devices and records are kept and maintained accurately by authorised personnel;

5.2.6 Responding to formal requests to access records, including law enforcement inquiries, in consultation with the Head Master, after consultation with the School's legal counsel;

5.2.7 Investigating privacy complaints related to video surveillance records, and security/privacy breaches;

5.2.8 Immediately reporting breaches of security/privacy to the Head Master and Board of Management or designate;

5.2.9 Reviewing annually the video surveillance system and policy and recommending updates as appropriate to the school management.

5.2.10 If required, preparing annual reports to the Group Operations (submitted through the Head Master) on all security video surveillance systems installed.

5.3 The Facilities, Health & Safety Manager

5.3.1 Is responsible for reviewing security and safety threat assessments to determine requirement for a video surveillance system;

5.3.2 Advising on installations and operation;

5.3.3 Assessing proposed installations in accordance with this Policy in consultation with the Head of Operations.

5.4 Head of ICT

5.4.1 Is responsible for all technical aspects of equipment, its installation and maintenance and the retention and disposal of the recorded information under consent of the Approvers.

5.4.2 Ensure all equipment lists are up to date.

5.4.3 Conducting periodic internal audits with the Head of Operations; to ensure compliance with this Policy.

- End of Policy -