SAHK B M Kotewall Memorial School
CCTV System Policy

1. The purposes underlying of CCTV system are as follows:
   1.1 To regulate school operations, safeguard the health and safety of students
   1.2 Prevention / detection of crime and unlawful activities.

2. Operation of CCTV system
   2.1 CCTVs are deployed and installed in indoor and outdoor public areas of the school premises, including but not limited to: school entrances, corridors, classrooms and activity rooms.
   2.2 The CCTV system within school premises operates 24 hours a day. All CCTV footages and data will be only retained for 30 days from the date of recording, and will be permanently deleted after this point.
   2.3 During the usage of CCTV system, the school employees will ensure students' privacy is maintained.
   2.4 The CCTV system is regularly inspected, repaired and maintained by the contractor in accordance with the Personal Data (Privacy) Ordinance and this policy.

3. Processing of CCTV footages
   3.1 Data Protection Measures
      3.1.1 The CCTV system and its operating system are located in the principal's office or within a locked room (according to the actual operation needs of the school, the operating system may be installed in a designated computer approved by the school).
      3.1.2 Only the principal, vice-principal, school management as well as (D1) domain supervisors in school have the password to access the system. The password will be changed when necessary.
      3.1.3 Data from the CCTV system are for authorized personnel's internal monitoring and investigation use only. In accordance to the Personal Data (Privacy) Ordinance, unauthorized persons are prohibited from viewing.
      3.1.4 The principal and authorized senior staff can view, download or copy the data captured from the system for internal use. If there is a need to download or copy the data, the storage device must be designated by the school with password-protected. Form PD31 must be completed for record.
      3.1.5 All authorized staff must properly keep the storage device containing the reproduced data. Within two weeks after the end of use, under the supervision of the principal / vice principal / management and (D1) domain supervisors as well as other authorized senior staff, the data is destroyed to an irreparable state.
      3.1.6 If the data is to be sent to a place outside the school, the storage device must be password-protected, and the staff authorized by the principal / vice principal shall deliver or transmit it under good security conditions, and fill in (Form PD33) for record.

3.2 Proper storage and use of data

3.2.1 Regularly viewing of data

For the purpose of monitoring the operation of the school, the principal, in collaboration with an authorized senior staff will randomly review no less than 10% of the school's video footage and at least 10 minutes of each video footage fortnightly. Each viewing will be of different time periods and different areas to ensure that students receive good services in a safe environment. All viewers are required to fill in (Form PD31), which is then kept securely by the school.

3.2.2 Spontaneous viewing of data

For the purpose of monitoring the operation of the school, the principal, in collaboration with an authorized senior staff will randomly review no less than 10% of the school's video footage and at least 10 minutes of each video footage at least 4 times a year. Each viewing will be of different time periods and different areas to ensure that students receive good services in a safe environment. All viewers are required to fill in (Form PD31), which is then kept securely by the school.

3.2.3 Viewing data as required

3.2.3.1 For security and investigation purposes, including but not limited to understanding the process of theft or irregular incidents, the principal and authorized senior staff can watch real-time images or review videos. In such situations, two authorized staff must watch simultaneously in school.

3.2.3.2 Under special circumstances, persons not authorized or appointed by the school (except for law enforcement agencies), such as government departments investigating an accident and requesting to view video recordings, or to transfer CCTV data, must apply and obtain formal approval from the principal before the reproduction of data, and (form PD33) is to be completed for record.

3.2.4 Properly keep viewing records: A record (Form PD31) must be completed for any viewing, downloading, copying or destruction of video data and shall be properly kept by the school.

4. Notification

4.1 The school has this policy at the reception desk, and since the CCTV system may capture personal images of students, parents, staff, visitors and the public, there is also a notice about the CCTV system at the reception desk (Appendix 1 and 2), so that all parties can understand the confidentiality principles and handling procedures of the school's use of the video recording system.

4.2 The school ensures all newly admitted students, their parents, and newly recruited employees understand the confidentiality principles and handling procedures of the school's use of the CCTV system.

4.3 Notices (Appendix 2) are posted outside the school to let the public know that the CCTV system is in operation.

5. Publication

5.1 This document is available at school for staff, parents and members of the public.

5.2 Any amendments to this document shall be announced at parent and staff meetings.

February, 2023