



CCTV SECURITY SYSTEM

DEFINITION: The installment of security cameras to regulate the management, operation and safety of the school, the staff, the parents and the students.

DESCRIPTION :

- The system comprises of 48 cameras.
- Cameras are installed in and around the school
- Cameras are not installed in classes or bathrooms
- This policy follows laws pertaining to Data Protection and Privacy, handling of evidentiary proceeding and the constitution of RSA 1996.

OBJECTIVES :

- To protect pupils, staff and visitors
- To increase personal safety and reduce the fear of crime.
- To protect the school buildings and assets
- Without prejudice, to protect the personal property of pupils, staff and visitors.
- To support the police in preventing and detecting crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To assist in managing the school.

STATEMENT OF INTENT

- The CCTV system will seek to comply with the requirements of the Laws pertaining to Data protection, privacy and handling of evidentiary proceedings and the Constitution of RSA 1996.
- The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- Cameras will be used to monitor activities within the school and its grounds to identify criminal activity actually occurring, anticipated, or perceived. It will be used for the purpose of securing the safety and wellbeing of the pupils, staff and school together with its visitors.
 - The system has been designed 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 have endeavoured to ensure that the system will give maximum effectiveness.
- Warning signs, as required by the Code of Practice of the laws pertaining to Data Protection, privacy and South Africa Intruder detection services association By-Law No.9, and Sec 14 of the Constitution of RSA 1996 will be clearly visible on the site.

SYSTEM MANAGEMENT

- The system will be administered and managed by the Principal and the Liaison Officer.
- The day to day management will be the responsibility of both the principal and the Liaison Officer.
- The system and the data collected will only be available to the Data Controller, the principal and the system manager.
- The system manager will check and confirm the efficiency of the system daily and in particular that the equipment is properly recording and that cameras are functional.
- 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 By-Law No.9 of South African Intruder Detection services association.
- The system manager must satisfy themselves of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists, access will be refused.
- Details including ALL visits and visitors will be recorded in the system log book including time/data of access and details of images viewed.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

DOWNLOAD MEDIA PROCEDURES

- In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -
 - Each download media must be identified by a unique mark.
 - Before use, each download media must be cleaned of any previous recording.
 - The system manager will register the date and time of the download media insertion, including its reference.
 - Download 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 download 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 download media is archived the reference must be noted.
- Images may be viewed by the police for the prevention and detection of crime and by authorised Forensic officers.
- A record will be maintained of the release of any download media to the police or other authorised applicants.
- Viewing of images by the police must be recorded in writing.
- Should images be required as evidence, a copy may be released to the police under the procedures described in the policy. Images will only be released to the police on the clear understanding that the download 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 download media (and any images contained thereon) to any other person. On occasions when a court requires the release of a download media this will be produced from the secure store, complete in its sealed bag.
- The police may require the school to retain the download media for possible use as evidence in the future. Such download media will be properly indexed and securely stored until they are needed by the police.
- Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the Board's Legal Department.

ASSESSMENT OF THE SYSTEM AND CODE OF PRACTICE

Performance monitoring, including random operating checks, may be carried out by the Principal or the Data Controller.

COMPLAINTS

Any complaints in relation to the school's CCTV system should be addressed to the Principal.

ACCESS BY THE DATA SUBJECT

- The data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.
- Requests for Data Subject Access should be made to the Principal or Legal Department of the school or the Data controller.

PUBLIC INFORMATION

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

SUMMARY OF KEY POINTS

- This policy will be reviewed every two years.
- The CCTV system is owned and operated by Principal.
- The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.

SIGNED AND CONFIRMED	
	
Mrs. M L Stander	Mrs. S van Zyl
Managing Director / Owner	Principal