Kaipaki School

CCTV POLICY

Purpose

The purpose of this Policy/(procedures) is to regulate the management, operation and use of the closed circuit television (CCTV) at Kaipaki School.

This Policy follows Privacy Act 1993 guidelines.

Objectives of the CCTV system:

To provide monitoring for the safety of students at school.
To protect the school buildings and their assets.

Statement of intent:

- All information, documents and recordings obtained and are protected by the Privacy Act.
- Cameras will be used to monitor the school entrance and classrooms for security and safety purposes.
- The addition of further cameras to the system or a change of area monitored will only happen with knowledge of the B.O.T. and adjustments made to this policy.
- Parents will be informed.
- Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- Warning signs, as required under the Privacy Act have been placed at all access routes to areas covered by the school CCTV.

Operation of the system:

- The system will be administered and managed by the Principal in accordance with the principles and objectives expressed in this policy.
- The day-to-day management will be the responsibility of the Principal.
- The ICT systems operator (iions) will be involved in maintaining security and system maintenance logs.
- If required, the systems licensed security installer (Sterling Security) may be called upon for assistance.
- The CCTV system will be operated 24 hours each day, every day of the year for the carpark camera, and 3pm until 8am in Ruma Rau and Ruma Peka during Term time (24 hours a day, every day of the school holidays).
- The security of the system will be monitored by iions and N4L, with a written report detailing security measures such as scans/firewalls given to the Board of Trustees annually.

Liaison:

Liaison meetings (to monitor and maintain the system) may be held with staff representatives, ICT systems operator (iions) and Security company (Sterling).

3. Monitoring procedures:

One monitor in the main server room by which pictures will be continuously recorded but not visible. The Principal may only access video footage through the security company (Sterling) or ICT operator (iions) with specific dates and times related to incidents under investigation.

The images are not stored on the cloud. If images are required for evidential purposes, the following procedures for their use and retention must be strictly adhered to:

- The images need to be transferred to a disk which must be sealed, witnessed, signed, dated and stored in a locked safe until collected.
- The disk should be new or cleaned of any previous recording.
- Disks may be viewed by the Police for the prevention and detection of crime or identification of a missing child.
- A record will be maintained of the release of disks to the Police or other authorised applicants. A register will be available for this purpose.
- Viewing of disks by the Police must be recorded in writing and in the log book.
- Requests by the Police can only be actioned through the principal/Board of Trustees Chairperson.
- Should a disk be required as evidence, a copy may be released to the Police. Disks will only be released to the Police on the clear understanding that the disk remains the property of the school, and both the disk and information contained on it are to be treated in accordance with this policy. The school also retains the right to refuse permission for the Police to pass to any other person the disk or any part of the information contained thereon.
- If a Court requires the release of an original disk this will be produced from the safe, complete in its sealed bag.
- The Police may require the school to retain the stored disks for possible use as evidence in the future. Such disks will be properly indexed and properly and securely stored until they are needed by the Police.
- Applications received from outside bodies (e.g. lawyers) to view or release disks will be referred to the Principal. In these circumstances disks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. 6.

Breaches of the policy (including breaches of security):

Any breach of this policy will be initially investigated by the Principal, in order to take the appropriate action and inform the board.
Any serious breach of this policy will be immediately reported to the BOT Chairperson and an independent investigation carried out to make recommendations on how to remedy the breach.

Assessment of the scheme and this policy:

Review of the effectiveness and appropriateness of ongoing use of CTV will be conducted tri-annually, with opportunity for community consultation where possible.

Complaints:

Any complaints about the school's CCTV system should be addressed to the Principal. Complaints will be investigated in accordance with the Complaints Procedures and with reference to this policy.

Access by the Data Subject:

The Privacy Act 1993 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.

Public information:

Copies of this Policy will be available to the parents from the School Office. A copy will also be available on the school website.

Summary of Key Points:

· The CCTV will be reviewed every three years.
· The CCTV system is owned and operated by the school.
· Liaison meetings may be held with the Police and other bodies.
· Video footage may only be viewed by Authorised School personnel, and the Police.
· Images required as evidence will be properly recorded on a disk from the Hard Drive, witnessed and packaged before copies are released to the police.
· Any breaches of this policy will be investigated by the Principal. An independent investigation will be carried out for serious breaches.
· Breaches of the policy and remedies will be reported by the Principal to the Board.

Security of the system will be constantly monitored, with annual written reports to the BOT detailing safety systems in place.