CCTV POLICY

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

This Policy follows Privacy Act 1993 guidelines.

Objectives of the CCTV system:
To protect the school buildings and their assets. The assets include the students, staff and our school community.

Statement of intent:
- All information, documents and recordings obtained and are protected by the Privacy Act.
- Cameras will be used to monitor the school grounds and buildings 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 will be involved in maintaining security and system maintenance logs.
- If required, the systems licensed security installer (Alliance Fire and Security) may be called upon for assistance.
- The CCTV system will operate 24 hours a day excluding the time when the school day is in operation; during this time, they will be non-operational. The school day is defined by the hours of 8:55am to 3pm
- The security of the system will be monitored by Postgate School.

Monitoring procedures:
One monitor in the main server room by which pictures will be continuously recorded but not visible.

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 or USB which must be sealed, witnessed, signed, dated and stored in a locked safe until collected.
- The disk/USB 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/USB 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/USB be required as evidence, a copy may be released to the Police. Disks/USB 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/USB this will be produced from the safe, complete in its sealed bag.
- The Police may require the school to retain the stored disks/USB 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/USB will be referred to the Principal. In these circumstances disks/USB 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.

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 on-going use of CTV will be conducted tri-annually or at any time with justification, 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, or at any time with justification- This may include, but not limited to, a known offender moving into the area.
- 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 (Principal. Deputy Principals, Board Chair, Property Manager), 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.

_____
Signed Board Chairperson

Review: _____

Camera Surveillance Guidelines

The school's camera surveillance system is installed to deter crime and undesirable behaviours, and thus provide greater protection for our students and staff, and less wilful damage to property. The system may operate 24 hours a day, seven days a week, according to the school's evaluation of when it is needed.

The school complies with the Privacy Act in using and managing the system and every effort is made to prevent it impacting on the privacy of the school community in its daily life. Specifically, the Privacy Act demands that:

- Information is only collected for a necessary and lawful purpose.
- Individuals must be aware of the information collection and the reason for it.
- Information collected for one purpose cannot be used for another.
- Information is stored and disposed of securely.

To achieve this, we have the following guidelines:

- The Principal is responsible for overseeing the CCTV system.
- The system is installed so that individuals committing a crime on school grounds can be identified and prosecuted. It is only used to identify persons illegally on the premises or engaged in criminal activity, or disturbing school programmes or individuals.
- Access is limited to the Principal and appointed system managers. A log book is used which details access to the system, the purpose of the access, and the operator.
- Staff are advised that while they go about their normal business at the school, their recorded images, and those of their students, will not be reviewed except to identify culprits.
- No recorded data is taken from the system unless approved in writing by the Principal
- Police may request access to CCTV records when investigating criminal activity in the area. The police are given access to the system as required but must comply with this policy. If the school has concerns about releasing this information, we will contact our legal advisors. The school must comply if the police have a search warrant.
- Requests for access to the system from parents or other interested parties will be denied unless good cause is given and the board formally approves this access.
- Any system misuse is reported to the principal, or the board of trustees if the principal is involved.
- We have signage in strategic places to inform people of the system, and our reason for it.
- Staff have the right to see footage of themselves as it is personal information held about them. However, they can only see it if it is readily retrievable, so must supply a time, date and location. The privacy of other people who may be in the footage must be considered in this case.
- All data, hard drives, etc., are destroyed or stored in compliance with the approved standard on data protection. Data is stored according to the standard so that it is not compromised and can be successfully used in court as evidence.
- Cameras are not installed in sensitive places such as bathrooms.

See the **Office of the Privacy Commissioner**, especially **Privacy and CCTV**, and **Privacy in Schools**.