CCTV POLICY

Version: 1.0
Approved: October 2015
Reviewed Date:
Amended:
Next review: October 2017

1. Introduction

1.1 The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Aparima College

1.2 The system will comprise of a number of fixed 'fish eye' cameras located around the school site. All cameras are monitored from the Deputy Principal's office, and access is only available to designated staff – members the Senior Leadership and Management Team

1.3 This Code follows Privacy Act 1993 guidelines.

1.4 The Code of Practice https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf (Privacy Commissioner, code of practice for CCTV) will be subject to review bi-annually to include consultation as appropriate with interested parties.

1.5 The CCTV system is owned by the school.

2. Objectives of the CCTV scheme

2.1

(a) To increase personal safety of students, staff and visitors and reduce the fear of bullying and crime.
(b) To protect the school buildings and their assets.
(c) To assist in identifying offenders.
(d) To protect the personal property of students, staff and visitors.

3. Statement of intent

3.1 The school will treat the system and all information, documents and recordings obtained and used as data which is protected by the Privacy Act.

3.2 Cameras will be used to monitor activities within the school and its car parks and other public areas to identify undesirable activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the school, together with its visitors.

3.3 Staff have been instructed that static cameras are not to focus on private/staff homes, gardens and other areas of private property.

3.4 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. CD images/disks will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. CD images/disks will never be released to the media for any other purpose.

3.5 The planning and design of the system endeavours to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.6 Warning signs, as required under the Privacy Act have been placed at all access routes to areas covered by the school CCTV.

4. Operation of the system

4.1 The Scheme will be administered and managed by the Deputy Principal or their nominee, in accordance with the principles and objectives expressed in the code.
4.2 The day-to-day management will be the responsibility of both the Senior Leadership & Management Team (SLMT) during the day and out of hours and at weekends.
4.3 The Server Room and Information Systems Directors office will only be accessed by SLMT, Information Systems Director and nominated staff.
4.4 The CCTV system will be operated 24 hours each day, every day of the year.

5. Server Room

5.1 The Information Systems technician (commissioned through SPARK Digital) will check and confirm the efficiency of the system fortnightly and in particular that the equipment is properly recording and that cameras are functional.
5.2 Access to the CCTV Server Room will be strictly limited to the SLMT, Information Systems technician and nominated staff.
5.3 Unless an immediate response to events is required, staff in the CCTV Server Room must not direct cameras at an individual or a specific group of individuals.
5.4 The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Principal and must be accompanied by a nominated staff member throughout the visit.
5.5 If an out of hours maintenance emergency arises, the Server Room Operators must be satisfied of the identity and purpose of contractors before allowing entry.
5.6 A visitor's book will be maintained at school reception. Full details of visitors including time/data of entry and exit will be recorded.
5.7 Other administrative functions will include maintaining hard disc space and occurrence and system maintenance logs (all logs will be maintained in the Deputy Principal's office).

6. Liaison

6.1 Liaison meetings (to monitor and maintain the system) may be held with staff representatives, ICT systems operator (SPARK Digital), the Schools SLT and the SMT who are directly involved in the support of the CCTV system.

7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.
7.2 Monitoring will be via a laptop computer which will remain in fixed position inside the Server Room.
7.3 All cameras operate using a Hard Disk for recording and the transfer of data from the HD to the Laptop will be overseen by the Deputy Principal.

8. Image storage procedures

8.1 The images are stored on the Hard Drive. If images are required for evidential purposes, the following procedures for their use and retention must be strictly adhered to:

i. The images need to be transferred to a disk which must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence disk store until collected.
ii. Each disk must be identified by a unique reference number.
iii. The disk should be new or cleaned of any previous recording.
iv. If the disk is archived at a later date, the reference number must be noted.

8.2 Disks may be viewed by the Police for the prevention and detection of crime.

8.3 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.

8.4 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 rector.

8.5 Should a disk be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (i) of this Code. 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 code. 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. On occasions when a Court requires the release of an original disk this will be produced from the secure evidence disk store, complete in its sealed bag.

8.6 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.

8.7 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.

9. **Breaches of the code (including breaches of security)**

9.1 Any breach of the Code of Practice by school staff will be initially investigated by the Principal, in order to take the appropriate disciplinary action.

9.2 Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the scheme and code of practice

10.1 Performance monitoring, including random operating checks, may be carried out by the Information Systems Technician.

11. Complaints

11.1.1 Any complaints about the school's CCTV system should be addressed to the Principal.

11.2 Complaints will be investigated in accordance with the schools complaints procedures in accordance with Section 9 of the Code of Practice.

12 Access by the Data Subject

12.1 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.

12.2 Requests for Data Subject Access should be made to the Principal.

13. **Public information**

Copies of this Policy and the Code of Practice will be available to the public from the School Office and the Principal.

Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the school.
- The Server Room will not be staffed out of school hours.
- The Server Room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the Police and other bodies.
- The Hard Drive may only be viewed by Authorised School Officers, Server Room staff 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.
- Disks will not be made available to the media for commercial or entertainment.
- Disks will be disposed of securely by incineration.
- Any breaches of this code will be investigated by the Principal. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Principal.