New Plymouth Girls' High School
Te Kura Taitamawāhine o Puke Ariki

5.7 SCHOOL AND HOSTEL SECURITY POLICY

Outcome statement

The School and Hostel's security system safeguards school assets against unlawful entry, wilful damage, burglary, and fire, while also deterring undesirable behaviour and improving student and staff safety.

Scope

The Board has oversight of the security systems and the management and review of those systems, to ensure that the School and Hostel are operating these in accordance with their purpose and this policy.

Delegations

The Board delegates overarching responsibility of the management of the School and Hostel's security systems to the Principal.
The School's Business Manager is responsible for overseeing the School's building alarm and fire alarm systems.
The School's Privacy Officer is responsible for overseeing the School's CCTV system.
The Hostel's Manager is responsible for overseeing the Hostel's security systems.

1. **Expectations and limitations**

a) School and Hotel staff members are always security conscious, and:
- Establish a challenge culture that stops and questions strangers on school grounds.
- Lock away valuable equipment such as laptops.
- Lock away personal valuables.
- Store valuable items out of sight, especially at weekends.
- Are responsible for locking rooms and areas as required.
- Report any suspicious activity.
- Report any loss of keys immediately.

b) The School and Hostel has a security surveillance system installed to deter unlawful entry, wilful damage, to discourage undesirable behaviours and improve student and staff safety. The School and Hostel follows guidelines to ensure that all aspects of the surveillance system, i.e. recording, management, access, storage, and access of recorded data, comply with the Privacy Act 2020 and guidelines provided by the Privacy Commissioner.

2. Security Alarm and Fire Alarm Systems

a) Alarm and Fire Alarm systems are monitored as appropriate.
b) Contact the alarm/security/fire safety company in the event of any accidental activation of

the alarm and quote the confirmation code (if known).

c) Where buildings are protected by an alarm, these are automatically activated on a timer.

d) When returning out of school hours, staff must disarm the alarm and notify the security company (if the alarm sounds). Failure to notify the security company leads to a call-out of security personnel. Staff must reset the alarm before leaving.

e) In accordance with the Fire and Emergency New Zealand Act 2017, it is an offense to knowingly give false alarm of fire (e.g., maliciously set off a fire alarm within the School or Hostel that creates a false or unwanted alarm). An offense of this kind is considered serious and will be treated through the school's student behaviour processes and the Police.

f) All key holders entering buildings after hours must check the security of the areas they are entering/exiting, whether alarmed or not.

3. Camera Surveillance (CCTV) Guidelines

a) The School and Hostel's camera surveillance system is installed to deter crime and undesirable behaviours and provide greater protection for our students and staff and to deter wilful damage to property.

b) The system may operate 24 hours a day, seven days a week, according to the School and Hostel's determination of when it is needed.

c) The School and Hostel complies with the Privacy Act 2020 in using and managing the system and every effort is made to prevent it impacting on the privacy of the School and Hostel community in its daily life.

d) 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.

e) To achieve this, the School and Hostel has the following guidelines:
- The system is installed so that individuals committing a crime or engaging in undesirable behaviours on school or hostel grounds can be identified and where appropriate, prosecuted or be subject to school student behaviour processes.
- It is only used to identify persons illegally on the premises or engaged in criminal activity, engaging in undesirable behaviours within the School or Hostel grounds or disturbing School programmes, Hostel life or individuals.
- Access to the system is very restricted and may be granted by the Privacy Officer for purposes that directly relate to an individual's job or role within the school.
- A logbook 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 or support incident investigations.
- No recorded data is taken from the system unless approved in writing by the Principal, upon recommendation by the Privacy Officer or Hostel Manager.
- 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, it will seek legal advice. The school must comply if the police have a search warrant.

- Any system misuse is reported to the Principal, or the Board if the Principal is involved.
- The School and Hostel will have signage in strategic places to inform people of the system, and the reason for it.
- Staff, students, and interested parties 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 provide a time, date, and location. The privacy of other people who may be in the footage must be considered in this case. The Principal will approve access to footage and in some instances, the Board may be called on to formally approve access.
- All data, hard drives, etc. are destroyed or stored in compliance using good practices and in accordance with the Privacy Act 2020. Data is stored according to this 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 bathroom stalls, but may be installed to survey washbasins, entrances to bathroom blocks or buildings, and signage will inform people that security systems are in the vicinity.
- The monitoring firm provides regular reports on the effectiveness of the system, and the system's operation is checked regularly by the Privacy Officer, Hostel Manager, and monitoring firm.
- The system, its operation, and related policies and procedures are audited and evaluated regularly as part of the annual health and safety audit.

4. Cybersecurity

To protect digital assets and personal information, the School and Hostel will have implemented robust cybersecurity measures. This includes regular updates to software and systems, secure password protocols, and staff training on cybersecurity best practices. The School's IT department is responsible for monitoring and managing cybersecurity threats and ensuring compliance with relevant legislation, such as the Privacy Act 2020. Where appropriate and possible two factor authentication should be implemented.

5. Community Involvement

The School and Hostel value the input and involvement of the school community in the development and review of security policies. Parents, caregivers, and students are encouraged to provide feedback and participate in consultations to ensure the policy meets the needs and concerns of all stakeholders.

Procedures/supporting documentation

Privacy and CCTV Guide - Privacy Commissioner

Privacy Policy

Online Safety Policy

Monitoring

The Principal will ensure that the School and Hostel's security systems are reviewed annually in accordance with Privacy Commissioner guidelines and health and safety audit requirements.

Legislative compliance

Privacy Act 2020
Fire and Emergency Act New Zealand 2017

Reviewed: February 2025	Next review: 2028