Clayfield College

CAMERA SURVEILLANCE AND VAPE DETECTION POLICY

1. RATIONALE

The use of Vape Detection Units and Camera surveillance footage shall be managed in accordance with this procedure and the collection and storage, use or disclosure of personal information shall be managed applying best practice principles in line with privacy obligations in the Information Privacy Act 2009 (Qld) and Privacy Act 1988.

2. SCOPE

This policy applies to all members of the College community.

3. POLICY STATEMENT

Clayfield College utilises camera surveillance systems which involves the collection and storage, use or disclosure of personal information for legitimate business activities.

Camera surveillance is utilised at the College to deter property crime, assist in the investigation and prosecution of criminal offences and to assist in the safe management of the College grounds, assets, and people. Camera Surveillance Systems may also be used to assist in investigation into child protection and student behavioural matters. Cameras have been placed outside the bathroom to monitor students entry and exist from the bathroom when the vape detectors have been triggered. Vaping poses a significant health risk and is prohibited at Clayfield College.

4. REFERENCES

4.1 References to other Policy

- *PMSA Privacy Policy*
- *PMSA Child Protection Policy*
- *Information Collection Notice Student*
- *Duty of Care – Student smoking, vaping and e-Cigarettes*
- *Contractor, Volunteer and Visitor Management Policy and Procedures*
- *Record retention schedule*

4.2 Legislative and other References

- *Information Privacy Act 2009 (Qld)*
- *Right to Information Act 2009*
- *Work Health and Safety Act and Regulations 2011*

Clayfield College

5. RESPONSIBILITIES

Principal

- Oversight of overall system.

Information Communication and Technology Manager

- Responsible for use of the Camera Surveillance System including the protection of the privacy interests of individual members of the College community and the public from intrusive monitoring.

6. GUIDELINES FOR STAFF

6.1 Any authorised persons involved in the recording, observation and retention of images shall be informed, through training by means of orientation to this procedure of their responsibility to act in an ethical and lawful manner as per the relevant legislation and this procedure.

If evidence is provided that an authorised or unauthorised individual is using the system inappropriately, the College will take appropriate measures to eliminate or minimise the risk of reoccurrence. Inappropriate and unauthorised use of the CCTV system will be considered a breach of the PMSA Staff Code of Conduct and will be managed accordingly.

6.2 Fit for Purpose

Cameras have been selected and positioned to ensure they only view areas relevant to the intended purpose. Cameras are located and positioned in a way that will not intrude to an unreasonable extent on the privacy of individuals.

6.3 Public Notification

All visitors to the site are informed of the presence of CCTV/Camera Surveillance via signage located at each of the site entrances. Parents are informed of CCTV Camera Surveillance during the admissions process and Staff within the Staff Handbook and at orientation.

In addition, the Visitor Information and Procedures outlines the presence of camera surveillance and reference to the Camera Surveillance Policy.

6.4 Personal Information

Personal information is any information or opinion, whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.

If the camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from footage. Footage will reveal information about that individual, for example, that they were present in that space at that time. As such, camera surveillance footage potentially contains personal information and obligations in the privacy principles apply.

6.5 Review and Retention of Footage

Footage shall only be accessed by persons authorised by the Principal. Access to footage shall be in accordance with their allocated duties. All requests and attempts and footage retention will be logged with the principal's office.

Matters involving student behavioral monitoring and child protection shall be undertaken as directed by the Principal.

Retention requests and grants shall be recorded for auditing purposes including:

- Name of person requesting footage – retention
- Time, date and for what purpose the footage retention request has been made
- Approval details from the principal's office

Footage shall only be used for the purposes for which it was obtained unless one of the following exceptions apply:

- Using it with the individual's consent
- Under a legislative authority for law enforcement purposes
- Prevent risks to health and safety under the Work Health and Safety Act and Regulations 2011

Where multiple footage exists of an individual involved in a specific incident that needs to be used for intended purposes, only the portions of the footage surrounding, or relevant to the incident may be used.

6.6 Storage and Disposal of Footage

Physical, technical, and operational safeguards shall be in place to ensure stored footage is protected against misuse, loss, and unauthorised access, use and disclosure.

Physical safeguards include placing cameras out of reach, using locks for access to control office and data storage areas, positioning monitors and screens so live footage cannot be viewed by unauthorised persons.

Technical safeguards include storing footage in encrypted form, encrypting any footage stored on portable storage devices.

Operational safeguards in place include the establishment of this documented procedure, limiting the number of staff who can access footage and or control rooms, restricting approval to access through the principal's office granting access.

Footage may be reviewed or stored post incident onsite for the purposes of investigation into any reported incident.

Camera Surveillance footage is overwritten or otherwise disposed of when it is no longer required by the College for its intended purpose. Camera Surveillance footage is stored for up to 30 days before being overwritten.

6.7 Liaison with Queensland Police Service (QPS)

Images may be released to QPS or other law enforcement agencies in compliance with the Information Privacy Act 2009 (Qld). All requests made by the QPS or other law enforcement agencies should be referred to the Principal who will arrange request management.

Matters involving child protection and student behaviour that involve notification and consultation with QPS and possible footage disclosure shall be overseen by the Principal.

6.8 Footage Disclosure

Should an incident occur, footage may be provided to Queensland Police Service for law enforcement purposes where the footage is deemed 'reasonably necessary' for a law enforcement activity.

Information will not be given to any other person or agency unless authorised or required by law or if applied for under the Right to Information Act 2009 or Chapter 3 of the IP Act. Where footage is disclosed for law enforcement or other purposes, a record of the disclosure shall be made and recorded along with the record of the request for disclosure.

6.9 Incident Report and Investigation

Security incidents shall be entered into Assurance reporting system where an incident involved damage to or the theft of property, assault or significant suspicious activity or is deemed a Health and Safety Risk.

Any incident which results in injury to an individual, assault of a staff member of any incident involving the brandishing or use of a weapon must be immediately reported to the Operations Manager.

The Operations Manager shall inform the Principal and Director of Corporate Services and coordinate follow-up action as appropriate, including liaising with law enforcement authorities etc.

Child protection and student behavioural matters shall be reported, recorded and investigated as per relevant policies.

6.10 Document Retention

Surveillance footage is retained no more than 30 days, unless archived due to reported incident.

Security documentation shall be retained in line with the Clayfield College Record Retention Guidelines for a period of 5 years.

7. DEFINITIONS

Nil

Clayfield College

Clayfield College

8. ATTACHMENTS

Nil

Version Control Table			
Version Control	**Date Effective**	**Approved By**	**Amendment**
1.00	October 2024	Principal	Creation of document
2.00	November 2024	Principal	Changes to viewing permission