Policy: Camera Surveillance

Policy Statement

At Jireh Christian School, surveillance practices comply with the Privacy Act 2020. Jireh Christian School ("the School") has undertaken a privacy impact assessment that informs the placement and use of cameras at the School. The purpose for implementing camera surveillance is to promote school safety and security, safeguard individuals and property, and facilitate investigations into unlawful, harmful, or unsafe conduct. The School's Privacy Officer is responsible for the camera surveillance system. The Privacy Officer is the Principal.

Procedural Guidelines

This policy is to be read in conjunction with the Privacy Act 2020 Policy.

Privacy Impact Assessment

Before introducing cameras into any area of the School, the impact on privacy as a result of using camera surveillance, including potential breaches of the Privacy Act 2020, was considered. In particular:

- the vulnerability of children and young people (Privacy Act 2020 s 22, Principle 4)
- the availability of other strategies to address security, behaviour, and safety issues (e.g., behaviour management plan)
- whether camera surveillance is necessary and proportionate to the issue being addressed
- cameras will not be installed in bathrooms, changing areas, counselling spaces, or other locations where individuals possess a reasonable expectation of privacy
- the risk that this surveillance breaches other legislation, such as the Human Rights Act 1993.

Purpose of Camera Surveillance

The School only collects information for a necessary and lawful purpose (Privacy Act 2020, Principle 1).

The purpose for using camera surveillance is to deter and identify anyone:

- entering the school grounds illegally
- engaging in unlawful, harmful, or unsafe behaviour
- engaging in conduct that places health and safety, school property, or school security at risk.

Camera surveillance will only be used for the purposes outlined in this policy and will not be used for staff performance management or routine student discipline monitoring.

Informing People about Camera Surveillance

Individuals will be made aware that the School is collecting information and the reason for collecting it (Privacy Act 2020, Principle 3). Signage will be clearly displayed at school entrances and in other relevant locations where surveillance is in place.

Questions, concerns, or requests regarding camera surveillance should be directed to the Principal, the Privacy Officer.

This Camera Surveillance Policy also acts as a privacy notice, which is made available on the School website under Policies and Procedures.

Storing and Securing Camera Surveillance Data

Privacy policies and information storage procedures are followed to ensure camera surveillance data is protected from loss, unauthorised access, use, modification, disclosure, and other misuse (Privacy Act 2020, Principle 5). All data is stored or destroyed in accordance with approved data protection standards.

Camera equipment and stored footage must be physically and electronically secured. Camera footage will only be retained for as long as necessary and will usually be deleted after a defined period, unless required for an investigation, legal matter, or official request. Any external provider involved in maintaining or monitoring the system must comply with the School's privacy and confidentiality requirements.

The School's information technology provider/monitoring firm will provide regular reports on the effectiveness of the system. The system's operation will be checked regularly by the Privacy Officer and the information technology provider/monitoring firm.

Any suspected misuse or privacy breach is reported to the Principal or the Board (if the Principal is involved) and will be investigated and managed in accordance with the School's Privacy Act 2020 Policy. The system, its operation, and related policies and procedures are audited, evaluated annually, and reported to the Board.

Accessing Camera Surveillance Data

The following conditions are assured when accessing or providing access to camera surveillance data:

- Access to camera surveillance data is limited to the Privacy Officer or their delegate, and appointed system managers, i.e. the Principal and Deputy Principal.
- Access must only occur for a legitimate school, safety, disciplinary, privacy, or legal reason.
- A record will be kept of who accesses the system and why.
- No data is removed from the system unless approved in writing by the Privacy Officer.
- If people are recorded during normal school activities, their recorded images are not viewed, and individuals are not identified unless there are reasonable grounds to view the footage and identify the individuals.
- No one is allowed to access camera surveillance data that does not contain their personal information.

However, people have the right to request access to camera surveillance data that includes their personal information (Privacy Act 2020, Principle 6). If providing access would reveal the personal information of another person, reasonable steps will be taken to protect the other person's privacy. It is likely that personal access will be limited to view-only in order to prevent unnecessary disclosure or publication of another person's personal information.

Any disclosure to the Police will be assessed in accordance with the Privacy Act 2020to ensure it is lawful, necessary, and proportionate.

Legislative Compliance

Regulations 8 & 9 Education (School Boards) Regulations 2020
Section 156 of the Education and Training Act 2020
Privacy Act 2020
School Cyber Safety Policy
Privacy Act 2020 Policy

Review schedule: Annually

ADOPTED BY BOARD

Date 19th May 2026 Presiding Member **A Coombridge**

Reviewed Date