



Riversdale School

Next review: Term 1 2027

Camera Surveillance Policy

At Riversdale School our camera surveillance practices comply with the Privacy Act 2020. Riversdale School has undertaken a privacy impact assessment that informs the placement and use of cameras at our school. We have a set purpose for camera surveillance, inform people about the surveillance, and ensure the data collected is stored and secured safely, and only accessed by authorised people. Our privacy officer is responsible for the camera surveillance system. Our privacy officer is the principal.

Privacy impact assessment

Before introducing cameras into any area of the school, we consider the impact on privacy as a result of using camera surveillance, including potential breaches of the Privacy Act. In particular, we consider:

- the vulnerability of children and young people (Privacy Act s 22, Principle 4)
- the availability of other strategies to address security, behaviour, and safety issues (e.g. behaviour management plan, smoke/vape detectors)
- whether the camera is positioned in a place where people would have a reasonable expectation of privacy (e.g. bathrooms, including entrances)
- the risk that this surveillance breaches other legislation such as the Human Rights Act 1993.

Purpose of camera surveillance

We only collect information for a necessary and lawful purpose (Principle 1). Our purpose for using camera surveillance is to deter and identify anyone:

- entering the school grounds illegally
- engaging in criminal activity, misconduct, or behaviour risking harm to health and safety.

Camera surveillance is not used to routinely monitor students or staff as this breaches the information privacy principles of the Privacy Act (Principles 4 and 10).

Informing people about camera surveillance

We make individuals aware we are collecting their information and our reason for collecting it (Principle 3). We use signage to inform people accessing our school grounds of the use of camera surveillance.

This Camera Surveillance Policy also acts as a privacy notice, which is made available to our school community on SchoolDocs. We inform our school community via the school website.

Storing and securing camera surveillance data


We follow our privacy policies and information storage procedures to ensure camera surveillance data is protected from loss, unauthorised access, use, modification, disclosure, and other misuse (Principle 5). All data (e.g. hard drives) is destroyed or stored to comply with approved data protection standards. See [Privacy Policy](#), [Computer Security and Cybersecurity](#), and [School Records Retention and Disposal](#).

We require our information technology provider/monitoring firm to provide regular reports on the effectiveness of the system. The system's operation is checked regularly by the privacy officer and information technology provider/monitoring firm. Any system misuse is reported to the principal or the board (if the principal is involved). The system, its operation, and related policies and procedures are audited, evaluated annually, and reported to the board.

Accessing camera surveillance data

We ensure the following conditions 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.
- We record 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 we have reasonable grounds to view the footage and identify the individuals.
- We do not allow people to access camera surveillance data that does not contain their personal information.

People have the right to request access to camera surveillance data that includes their personal information (Principle 6). If providing access would reveal the personal information of another person, we take reasonable steps to protect the other person's privacy. It is likely that personal access will be limited to view-only to prevent unnecessary disclosure or publication of another person's personal information. See [Personal Information](#) and [Responding to access requests for CCTV footage](#)  (Privacy Commissioner).

Police may request access to camera surveillance data when investigating criminal activity. We do not have to provide access but we may if we are reasonably satisfied that this will not breach privacy principles and will help the police with the prevention, detection, investigation, prosecution, and punishment of offences. If police require release we cooperate as appropriate. See [Sharing Student Personal Information with External Agencies](#).

Related policies

- [Privacy Policy](#)
- [Personal Information](#)
- [Computer Security and Cybersecurity](#)
- [School Records Retention and Disposal](#)

Legislation

- Privacy Act 2020

- Human Rights Act 1993
 - Search and Surveillance Act 2012
-

Resources

- Privacy Commissioner | Te Mana Mā tā pono Matatapu:
 - [Privacy and CCTV](#)
 - [Privacy Impact Assessments](#)
 - [CCTV and school bathrooms](#)
- GCSN: [Cyber Safety Action Plan](#)

Release history: Term 1 2024, Term 2 2021, Term 1 2021, Term 4 2020

Last review	Term 1 2024
--------------------	-------------