

CCTV policy

Schools of Otamatea Network Group and Leabourn Passenger Services

About this policy

The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) on school buses provided by the Schools of Otamatea Network Group ("the Group"). This policy follows Privacy Act 2020 guidelines.

The parties referred to in this policy are:

- Network Manager: the person responsible for managing the school bus network on behalf of schools
- Network Chair: the Chairperson of the Group's Committee
- Principal: a principal of one of the four schools that comprise the Group
- Deputy Principal: the Deputy Principal of Otamatea High School
- Investigating Person: a manager from the bus operator or a school tasked with investigating a complaint.

1. Objectives of the CCTV System

- 1.1. To improve the safety of students at whilst on and around the school bus
- 1.2. To improve the behaviour of students by presenting a visible deterrent
- 1.3. To assist in the resolution of complaints made against the driver or students
- 1.4. To protect the bus operator's assets.

2. Statement of Intent

All information, documents and recordings obtained and are protected by the Privacy Act. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Warning signs, as required under the Privacy Act, have been placed at access points on the vehicle.

3. Operation of the System

The system will be administered and managed by the Network Manager in accordance with the principles and objectives expressed in this policy. If required, the CCTV system's installer may be called upon for assistance.

4. Liaison

Liaison meetings (to monitor and maintain the system) may be held with school representatives, Leabourn Passenger Services, the system installer (QuickStart) and the Network Manager.

5. Monitoring Procedures

The Network Manager, Principals and Deputy Principal will have access to monitor all cameras on their computers.

6. Data Storage

The data is processed by the Digital Video Recorder (DVR) on each bus. Data is stored on a Hard Disk Drive attached to the DVR for approximately one month before being over-written by newer data. Video and audio data is recorded.

7. Accessing live data

The data may be accessed via a 3G/4G connection to the DVR for the purposes of addressing any real-time concern about service delivery. Recordings will not be made of live data.

8. Access Procedures when investigating an event

If data is required for evidential purposes, the following procedures for the use and retention must be strictly adhered to.

- The Investigating Person will complete the CCTV Data Access Form and submit it to the Network Manager, who will consult with the Network Chair as appropriate
- The data will be transferred from the DVR by the Network Manager to an encrypted folder on the Google Drive at Otamatea High School
- The data will be stored in a folder discrete from other data
- The Network Manager will email a link to the folder to the Investigating Person
- Once the complaint has been resolved, the data will be deleted
- A log of data requests will be maintained by the Network Manager.

9. Authority to view data

The only parties authorised to view data copied for evidential purposes are the Network Manager, Principals, Deputy Principal and a person completing an investigation (Investigating Person). In the event of a complaint against a bus driver, the Investigating Person will be Lyndon Leabourn. In the event of a complaint against a student, the Investigating Person will be the Principal or Deputy Principal of the school that the student attends.

If the Investigating Person wishes the subject of the complaint, or their parent or guardian in the case of a student complaint, to view the data, they will request this in writing to the Network Manager. In making this request, the Investigating Person will note the parties that will view the footage.

The Network Manager will maintain a log of data requests and the parties that view them.

8. Requests by the Police and other bodies

Request by Police can only be actioned through a Principal. Should footage be required as evidence, a copy may be released to the Police. Released data will be provided on a USB flash drive. Footage will only be released to the Police on the clear understanding that the footage remains the property of the Group, and both the footage and information contained on it are to be treated in accordance with this policy. The Police may require the Group to retain the stored footage for possible use as evidence in the future. Such footage will be properly indexed and properly and securely stored in the Google Drive of Otamatea High School until they are needed by the Police.

Applications received from outside bodies (e.g. lawyers) to view or release footage will be referred to the Principal. In these circumstances footage will normally be released where satisfactory documentary evidence is produced showing that it is required for legal proceedings, a subject access request, or in response to a Court Order.

9. Breaches of the Policy (including Breaches of Security)

Any breach of this policy will be initially investigated by the Network Chairperson, in order to take the appropriate action and inform the Committee. Any serious breach of this policy will be immediately reported to the BOT Chairperson of an affected school and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment of the scheme and this policy

Performance monitoring, including random operating checks, may be carried out by the Network Manager, Principal, Deputy Principal and the system's supplier.

11. Complaints

Any complaints about the school's CCTV system should be addressed to the Network Manager. Complaints will be investigated in accordance with the Group's complaints procedures and with reference to this policy.

12. Access by the Data Subject

The Privacy Act 2020 provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to the Network Manager.