

# CCTV Surveillance Policy

**Responsibility for policy:** Chief Operating Officer

**Approving authority:** Vice-Chancellor

**Last reviewed:** July 2019

**Next review:** July 2024



## Application

1. This policy applies to all staff, students and visitors to the University of Waikato.

## Scope

2. This policy applies to all CCTV systems owned and/or operated by the University of Waikato at its Hamilton and Tauranga campuses and other satellite premises, including University of Waikato student accommodation and recreation facilities.
3. This policy does not apply to:
  - a. CCTV systems installed by retail or commercial tenants on the Hamilton or Tauranga campuses and other satellite premises
  - b. the recording of lectures and other teaching and learning activities and the subsequent use of such recordings, e.g. via Panopto
  - c. the use of video recording for video conferencing purposes, or
  - d. the use of live web-streaming cameras installed for public interest viewing, i.e. web cams.

## Purpose

4. The purpose of this policy is to:
  - a. provide information on the use of CCTV systems to deter and reduce the incidence of crime and disorder on University of Waikato campuses
  - b. outline the CCTV system monitoring processes in place that enable preventative or responsive actions to be taken as appropriate
  - c. assure staff, students and visitors to University of Waikato campuses of the safety measures that operate across those campuses within the context of applicable New Zealand legislation and industry best practice
  - d. set out principles, operational rules and responsibilities with respect to the collection, use and disclosure of images captured by CCTV systems on University premises.

## Related documents

5. The following documents set out further information relevant to this policy:
  - [Code of Student Conduct](#)
  - [Crimes Act 1961](#)
  - [Health and Safety at Work Act 2015](#)
  - [Human Rights Act 1993](#)
  - [Personal Information and Privacy Policy](#)
  - [Private Security Personnel and Private Investigators Act 2010](#)
  - [Privacy Act 2020](#)
  - [Privacy and CCTV: A guide to the Privacy Act for business, agencies and organisations](#) (Privacy Commissioner)
  - [Staff Code of Conduct](#)
  - [University of Waikato Privacy Statement](#)

## Definitions

6. In this policy:
  - access control** means an electronic or manual process used to control access to a building or site
  - closed circuit television (CCTV)** means a camera surveillance system that transmits and records images
  - University of Waikato student accommodation** means a hall of residence, apartment or other student accommodation owned and/or operated by the University.

## Principles

7. The purpose of CCTV systems on the University's campuses is to:
  - a. enhance the safety of staff, students and visitors to the University of Waikato
  - b. enable monitoring and surveillance to assist with the prevention, detection and investigation of criminal behaviour, including the identification and apprehension of persons committing offences on or around campus
  - c. protect University owned and/or operated property, buildings and critical infrastructure
  - d. assist with monitoring and enforcement of traffic related incidents on the campus
  - e. assist in the investigation of suspected breaches of University policy and codes of conduct by staff or students
  - f. verify identification for the purposes of access control to University buildings and to alert authorised security personnel of persons of interest who could potentially present as a threat to the safety and wellbeing of staff, students and visitors
  - g. provide data analytics to enhance the operational effectiveness of the University through improved building management systems, energy consumption and environmental best practice, and
  - h. monitor the assembly and movement of people around campus to assist with campus development planning.

## CCTV systems

8. CCTV systems in use on University campuses comprise a range of fixed-position cameras, pan tilt and zoom cameras, motion-activated recorders, monitors, digital recorders and public information signs.
9. CCTV images and recordings are stored on secure servers in a secure location and are accessible by authorised personnel only.
10. CCTV systems operate 24 hours per day, 365 days per year.

## Placement of CCTV cameras and field of view

11. CCTV cameras are located at various places on University premises and may be relocated from time to time.
12. With exception of temporary covert camera installations installed in accordance with clauses 19 to 22 of this policy, signs advising of CCTV cameras must be clearly displayed at all key pedestrian and vehicular entrance points to the University and buildings where cameras are in operation to ensure that staff, students and visitors to the University are aware that they are entering an area that is covered by CCTV surveillance (examples of CCTV signage are provided in the Appendix of this policy).
13. CCTV cameras may be installed inside and/or outside University buildings.
14. CCTV cameras are sited to cover the University premises as far as is possible, including:
  - a. roadways
  - b. carparks
  - c. buildings used for teaching, research and administrative purposes
  - d. student accommodation (entrances and communal areas only) and recreation facilities
  - e. licensed premises and
  - f. other vulnerable public areas.

15. CCTV cameras may cover (but are not limited to):
  - a. emergency phone locations
  - b. atrium social learning spaces
  - c. general circulation areas, corridors, hallways, pathways and key entrances to University campuses
  - d. areas where cash, high value equipment and high value information are stored or handled
  - e. areas where staff interact with students and/or the public (but not in individual offices)
  - f. areas with high risk equipment, processes or chemicals, e.g. laboratories
  - g. car parks and bike racks.
16. CCTV cameras must not be installed in any manner which impedes on the personal privacy of an individual; cameras must not be installed in:
  - a. toilets
  - b. showers
  - c. individual offices
  - d. private student residential rooms.
17. CCTV cameras must not be installed in any manner which records sound or audio.
18. CCTV cameras must not be installed in any manner which records information deemed commercially sensitive or information used in research activities.

#### **Temporary covert camera installations**

19. Where justifiable under the [Privacy Act 2020](#), such as in connection with a criminal investigation or to investigate issues that pose a significant threat to the operations of the University, the Vice-Chancellor may authorise temporary covert camera installations on University premises.
20. In accordance with clauses 16 to 18 of this policy, covert camera installations must not be installed in any manner which impedes on the personal privacy of an individual or commercial or research sensitivity.
21. The use of covert cameras to monitor staff performance is not permitted.
22. CCTV cameras will be removed immediately upon conclusion of any investigation.

#### **Access to, security and use of CCTV images and recordings**

23. CCTV installation, operation, monitoring and recording is undertaken by authorised personnel (staff and a contracted service partner) in compliance with relevant legislation and policy.
24. CCTV cameras are monitored from restricted control rooms and/or via University of Waikato mobile devices by authorised personnel.
25. The normal length of storage of CCTV images and recordings may vary between 30 and 90 days; information collected for evidential purposes may be retained and stored beyond this period.
26. In the event of unlawful activity being carried out on University premises and it being recorded by the University's CCTV systems, the University may pass that footage over to the Police for the purpose of an investigation.
27. If the Police believe that unlawful activity may have been carried out outside University premises that may have been captured on University CCTV systems, or if alleged offenders may have been captured on CCTV passing through University grounds, they may view or ask the University to provide any footage that may help.
28. Any individual who has been recorded by the University's CCTV has the right to access that footage so long as that information relates only to that individual; an individual has no right to access footage that does not relate to the individual.
29. Where a suspicion of staff misconduct arises, the Campus Security and Emergency Manager may provide access to CCTV images or recordings for use in staff disciplinary cases.
30. Where a suspicion of student misconduct arises, the Campus Security and Emergency Manager may provide access to CCTV images or recordings for use in student disciplinary cases.

31. All requests for access to CCTV images or recordings by staff or students must be made in writing to the Campus Security and Emergency Manager using the [Application for Access to CCTV Images](#) form.
32. All third party requests (such as by the Police or other public sector agencies) must be made in writing to the Campus Security and Emergency Manager and must be accompanied by the relevant order (such as a production order or court order).
33. Access to CCTV images or recordings may be refused on the grounds set out in Part 4 of the [Privacy Act 2020](#).
34. All requests for access to CCTV images or recordings must be responded to within 20 working days.
35. Access given to CCTV images or recordings is for the purpose for which it is granted only; images or recordings must not be distributed or published in any way.
36. If a request for access to CCTV images or recordings is unable to be granted without unreasonably breaching the privacy of other persons, a written description may be provided of activities in the footage pertaining to the individual requesting the information instead.
37. Data analytics information gathered from CCTV systems, such as parking data, may be provided to authorised staff for further analysis with a view to understanding and improvising logistical operational efficiencies.
38. All CCTV images and recordings remain the property of the University of Waikato.

### **Responsibilities**

39. The Vice-Chancellor is accountable for the provision and maintenance of a safe and healthy environment, and delegates relevant responsibilities with respect to CCTV systems to the Chief Operating Officer and the Campus Security and Emergency Manager.
40. The Chief Operating Officer is responsible for the overall management and operation of the CCTV systems, including the authorisation of staff for the monitoring of the cameras and recorded data.
41. The Campus Security and Emergency Manager is responsible for:
  - a. the installation, administration, monitoring and use of the University's CCTV systems
  - b. deciding the operating hours and locations of CCTV
  - c. ensuring that staff, students and visitors to the University are aware of the presence of CCTV, where it operates
  - d. the training of authorised personnel in the implementation of this policy
  - e. ensuring that the University complies with the [University of Waikato Privacy Statement](#), the [Personal Information and Privacy Policy](#) and the [Privacy Act 2020](#).
42. Authorised security personnel are responsible for taking the appropriate actions in relation to incidents captured by the CCTV systems.

### **Complaints**

43. Any person who believes that this policy has been breached is encouraged to advise the Chief Operating Officer who will investigate the matter.

### **Responsibility for monitoring compliance**

44. The Chief Operating Officer is responsible for monitoring compliance with this policy and reporting any breaches to the Vice-Chancellor.
45. Breaches of this policy by staff may result in disciplinary action under the [Staff Code of Conduct](#).
46. Breaches of this policy by student may result in disciplinary action under the [Code of Student Conduct](#).

Examples of CCTV signage in use at the University of Waikato

