Video Surveillance Camera Usage Policy

Policy #:	7.2
Current Publication Date:	May 2010
Previous Publication Date(s):	NEW Policy
Office of Accountability:	Campus Services & Security
Administrative Responsibility:	Director, Campus Services & Security
Approver(s):	Vice-President, Finance & Administration

1. Purpose

This policy provides guidance in the responsible use of video surveillance on OCAD University ("OCAD U" or "the University") premises. The purposes of video surveillances are to:

- Enhance the safety of OCAD U students, staff, faculty and general public;
- Protect University property against theft, vandalism and other criminal activity;
- Aid in the identification of intruders and other persons breaking the law.

Information obtained through video surveillance will be used exclusively for security and law enforcement purposes, which must relate to the protection of students, staff, faculty, and the public, or the deterrence or detection of criminal activity, including theft, vandalism, or other property damage.

OCAD U is committed to enhancing the University community's quality of life by integrating the best practices of security with the responsible use of technology.

Under the *Ontario College of Art & Design Act, 2002,* s.4(1), the University has the authority to collect personal information for the purposes of campus security.

Information must not be retained or used for purposes other than those described in this policy.

2. Scope

This policy has been created in accordance with the *Guidelines for Using Video Surveillance Cameras in Schools* as issued by the Information and Privacy Commissioner/Ontario, December 2003 and the Ontario *Freedom of Information and Protection of Privacy Act* (the *Act*), both of which outline the obligations imposed on institutions with respect to the protection of the privacy interests of individuals.

This policy is not intended to deal with instances where University staff videotape classes or specific events (such as visiting artists & lecturers), or when video is used as a medium for creative expression, or educational or research purposes.

It is also important to note that this policy does not apply to "covert surveillance." Covert surveillance refers to surveillance conducted by means of hidden devices, without specific notice to the individuals being monitored (see Appendix A – Covert Surveillance).

3. Policy

- Video monitoring of OCAD U premises will be conducted in a professional, ethical and legal manner.

- Video surveillance will be used only by University Security (i.e., not by others in the OCAD U community), and only where less intrusive means of deterrence, such as monitoring by Security staff, has been shown to be ineffective or unworkable.

- Video surveillance programs will be used only where circumstances have shown that it is necessary for the purposes of enhancing the safety of students and staff, or for the deterrence of theft or destructive acts, such as vandalism and graffiti.

- Video surveillance will be designed and operated in a manner that minimizes privacy intrusion and which is absolutely necessary to achieve its required lawful goals.

- University employees and service providers will have access to information collected under the program *only* in accordance with this policy, where necessary in the performance of their duties, and where the access is necessary and proper in the discharge of the University's functions. Any employee who knowingly or deliberately breaches this policy or the *Act* will be subject to discipline.

- Any employee who may need to access information collected under the video surveillance program will be provided proper training and orientation with regards to this Policy and the employee's obligations under this Policy and the *Act*.

- Video surveillance for the purpose of monitoring work areas, social areas, or sensitive areas will only occur in special circumstances, and must be in compliance with the policy's principle purpose, which include the prevention/deterrence of illegal activity and the enhancement of safety.

- Video surveillance will not be used for monitoring employee performance.

- If cameras are adjustable by operators, this practice will be restricted, wherever possible, so that operators cannot adjust or manipulate the cameras to view spaces that are not intended to be covered by the video surveillance program.

- Video surveillance will not be used inside areas where students, employees and the public have an unusually high expectation of privacy (e.g. in washrooms and change rooms).

- Students, staff and the public will be notified, using clearly written signs, displayed at the entrance to all premises, so that each person has reasonable and adequate warning that surveillance is, or may be, in operation.

- Signage about University video surveillance will make clear that cameras are not actively monitored. (For greater clarity, this is to ensure that OCAD U students, employees and visitors

are not lulled into a false sense of security, in the belief that help will automatically be on the way in an emergency situation).

- No attempt will be made to alter any part of a recording.

- Viewing of the recorded information will be limited to the following authorized University personnel:

    - Security Coordinator
    - Manager, Campus Security
    - Director, Campus Services & Security
    - Vice-President, Finance & Administration
    - President
    - And other persons with specific expertise which is directly relevant to an investigation, as approved by the Vice-President, Finance & Administration.

- Where a review of record information indicates that unlawful activity has occurred or is suspected, law enforcement agencies will be brought in to view that recorded information.

- When a recording is seized as evidence, the name of the investigating officer and date and time of seizure will be recorded and retained in a log book.

- All storage devices (such as CDs or hard drives) that are not in active use will be stored securely in a locked cabinet in a controlled-access area.

- Storage devices that are in continuous use will be overwritten on a regular basis, on a varying period of time, depending on the activity level and that period will generally not exceed thirty (30) days.

- Copies which are made of specific segments of recorded information for purposes of criminal investigation will be dated and labeled with a unique, sequential number or other verifiable symbol, and access to these copies will be limited to authorized personnel. Logs will be kept of all instances of access to, and use of, these stored copies, to provide for a proper audit trail. These stored copies will be retained for a period of one year as per section 5(1) of Ontario Regulation 460 under the *Act*. The length of this retention period may be reduced by way of formal resolution by the university or the courts.

- Any deviation from this policy will occur only with the explicit approval of the President, or designate.

- The university will review and evaluate this policy periodically, at least once every three years, in order to:

    - Accommodate developments in the interpretation of data protection legislation
    - Response to developments in the technology involved with the recording of images and the use of such technologies; and
    - Ensure that the procedures comply with all applicable laws and university policies, including laws and policies relating to privacy and access to information.

Appendix A – Covert Surveillance

Covert surveillance occurs when surveillance cameras are set up without notification. Because covert surveillance takes place without specific notice to the public, individuals are not generally aware that they are being monitored. As such, covert surveillance has the potential of being privacy-invasive and should therefore be used only as a last resort, in limited, case-specific circumstances.

Covert surveillance will be utilized by OCAD U only in extreme cases where it is the only available option under the circumstances, and when the benefits derived from the information obtained would far outweigh the violation of privacy of the individuals observed. In all cases, covert surveillance will be time-limited.

Camera equipment will be positioned in a way that minimizes unnecessary surveillance (e.g. in the case of an ongoing computer theft problem, the camera will be positioned so that individuals will be recorded only if they approach the equipment of concern). In most cases, the camera will be positioned to view entrances or exits to areas, rather than individual work stations. After a suspect has been identified, the surveillance equipment will be deactivated and/or removed as soon as possible.

Covert surveillance will not be used inside areas where students, employees and the public have an unusually high expectation of privacy (e.g. in washrooms and change rooms).

The decision to use Covert Surveillance will be made on a case-by-case basis, as approved by the Vice-President, Finance & Administration, upon recommendation from the Director, Campus Services & Security.